ON THE EQUIVALENCE OF QUADRATIC FORMS

By

THOMAS ROSCOE HORTON

A DISSERTATION PRESENTED TO THE GRADUATE COUNCIL OF
THE UNIVERSITY OF FLORIDA
IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE
DEGREE OF DOCTOR OF PHILOSOPHY

UNIVERSITY OF FLORIDA
August, 1954

ACKNOWLEDGMENTS

The writer wishes to express his sincere appreciation to Professor Edwin H. Hadlock, Chairman of his Supervisory Committee, for a generous contribution of time, energy, and helpful criticism throughout the preparation of this work and to Professors W. R. Hutcherson, F. W. Kokomoor, Z. M. Pirenian, and R. O. Stripling, all of whom served as members of his Supervisory Committee. To Professor Hadlock is due a large measure of gratitude for sympathetic encouragement and guidance during the author's entire doctoral program. Finally the author wishes to acknowledge that without the help of his wife, Marilou Horton, his graduate studies could not have been begun and that without her continued confidence in him his graduate studies could never have been completed.

TABLE OF CONTENTS

TABLE OF CONTENTS--Continued

LIST OF TABLES

CHAPTER I

INTRODUCTION

Historical Remarks

The notion of equivalence is a basic concept in the study of the arithmetic theory of quadratic forms, which itself is a branch of number theory. The study of quadratic forms may be said to have been initiated by Pierre de Fermat in 1654.[1] Since that time notable contributors have been, among others, Joseph Lagrange, Carl Friedrich Gauss, G. L. Dirichlet, G. Eisenstein, Henry J. S. Smith, and Leonard E. Dickson. The last-named has compiled an exhaustive history of the field in his Quadratic and Higher Forms, Volume III of the monumental three-volume History of the Theory of Numbers.[2] This work consists of a detailed, documented record of the results of research in the field of quadratic forms together with clear summaries of those results and in some cases sketches of the methods of proof of the results. As a field of mathematics number theory is unique in that such a precise, lucid, and thorough history is available to the research worker.

---

[1] L. E. Dickson, History of the Theory of Numbers, Vol. III, Quadratic and Higher Forms, (Washington,) 1923, p. 1.

[2] Ibid.

A recent exposition on some of the modern aspects of the study of quadratic forms has been published by The Mathematical Association of America as a Carus Mathematical Monograph, namely, The Arithmetic Theory of Quadratic Forms, by Burton W. Jones.[3] Number theorists engaged in research on forms owe much both to Dickson and to Jones for their successful and independent labors in systematizing and unifying their branch of mathematics. Although the results of researches into the properties of quadratic and higher forms have been extensive enough to fill, even in Dickson's concise style, three hundred pages of the History of the Theory of Numbers, Professor Jones remarks that "the theory of quadratic forms is rather remarkable in that, though much has been done, in some directions the frontiers of knowledge are very near."[4]

In this tercentenary year of the study of quadratic forms, it seems to the author especially appropriate that such an elemental and salient notion as equivalence be studied anew; it is hoped that by such a study the frontiers of knowledge will have been in some measure extended.

Definitions

A form is a homogeneous polynomial expression in two

---

[3] B. W. Jones, The Arithmetic Theory of Quadratic Forms, (Baltimore,) 1950.

[4] Ibid., p. viii.

or more variables. A <u>quadratic form</u> is a form of the second degree. A form of the second degree in n variables is called an <u>n-ary quadratic form</u> (<u>e.g.</u>, <u>binary quadratic form</u>, <u>ternary quadratic form</u>) and is thus a polynomial of the type

$$P(x_1, x_2, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij}x_i x_j .$$

When $a_{ji} = a_{ij}$, $i,j=1, 2, \ldots, n$, then P is said to be a <u>classic form</u>. In this dissertation the major emphasis is on classic, ternary quadratic forms, <u>i.e.</u>, only those quadratic forms which are in three variables and whose terms $x_i x_j$, $i \neq j$, have even coefficients. Henceforth the word <u>form</u> will denote a classic, ternary quadratic form unless it is stated otherwise.

The form

$$f = \sum_{i,j=1}^{3} a_{ij}x_i x_j \quad , \qquad a_{ji} = a_{ij},\ i,j=1,2,3,$$

is the general classic, ternary quadratic form. The coefficients of f are said to have the <u>matrix</u>

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix} .$$

With the form f there is associated the determinant $d = |a_{ij}|$. Let A_{ij} be the cofactor of a_{ij} in (a_{ij}). Then the form $\phi(x_1, x_2, x_3)$, defined as

$$\phi(x_1, x_2, x_3) = \sum_{i,j=1}^{3} A_{ij}x_ix_j,$$

is called the <u>adjoint form</u> of f or the <u>adjoint</u> of the form f.

A linear integral <u>transformation</u>

$$\begin{aligned} x_1 &= c_{11}y_1 + c_{12}y_2 + c_{13}y_3 \\ x_2 &= c_{21}y_1 + c_{22}y_2 + c_{23}y_3 \\ x_3 &= c_{31}y_1 + c_{32}y_2 + c_{33}y_3 \end{aligned}$$

is for brevity and convenience usually written as a matrix (c_{jk}), where

$$(c_{jk}) = \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \\ c_{31} & c_{32} & c_{33} \end{pmatrix}.$$

When a form f is subjected to such a transformation (c_{jk}) of determinant $|c_{jk}| = 1$ (or -1), then the resulting form f' is said to be <u>equivalent</u> (or <u>improperly equivalent</u>) to f. The form f' is a ternary quadratic form in the variables y_1, y_2, and y_3.

Let τ denote the g.c.d. (greatest common divisor) of the literal coefficients a_{ij} of f. Let σ denote the g.c.d. of its coefficients a_{11}, a_{22}, a_{33}, $2a_{12}$, $2a_{13}$, $2a_{23}$. Then if $\tau = 1$, the form f is said to be <u>primitive</u>. Evidently $\sigma = 1$ or 2. When $\sigma = 1$, f is said to be <u>properly primitive</u>; when $\sigma = 2$, f is said to be <u>improperly primitive</u>.

When x_1, x_2, x_3 are integers, the value of $f(x_1,x_2,x_3)$

is some integer m. Then m is said to be <u>represented</u> by the form f. If the g.c.d. of the three x_i is one, then m is said to be <u>represented primitively</u> by f or <u>represented properly</u> by f; the latter two terms are interchangeable, but throughout this study the former of the two will be used exclusively.

Statement of the Problem

The notion of equivalence is the central study of this dissertation. By the very definition of equivalence one may, given any form, produce an equivalent form by subjecting the original one to a unimodular transformation, <u>i.e.</u>, a transformation of determinant one. Conversely, if the resulting form and the transformation be known, then the original one may be obtained by elementary means. A problem arises, however, if this question is posed: given two forms of the same determinant, find the unimodular transformation, if any, which sends one into the other. This question and even the question of determining whether such a transformation exists possess no general answer. In other words, given two forms, are they equivalent? To obtain a partial answer to this last query, the major problem of this dissertation is as follows: what are some necessary and/or sufficient conditions that a form

$$f = \sum_{i,j=1}^{3} a_{ij}x_ix_j, \qquad a_{ji} = a_{ij} ,$$

of determinant $d \neq 0$, be equivalent to a form

$$f' = \sum_{s,k=1}^{3} b_{sk} y_s y_k$$

of a particular type? These types are based upon various restrictions which are placed upon the coefficients b_{sk} of f'. These restrictions may be found in subsequent chapter headings, in the statements of propositions, and in the summary. The viewpoint of the writer in seeking the conditions for equivalence was that if enough conditions could be found, then applications of proper combinations of the results might serve as useful tests for equivalence of particular forms. This conjecture proved to be true. During the course of the research several related questions presented themselves and were studied.

Results of the research are given in the form of mathematical statements --- lemmata, theorems, and corollaries, together with the proofs of these results. At the end of most chapters representative examples are offered.

CHAPTER II

CONDITIONS FOR EQUIVALENCE TO THE FORM f' WITH $b_{13} = 0$, $b_{23} = Kb_{33}$

When a ternary quadratic form is subjected to a linear integral transformation of determinant one, the coefficients of the resulting equivalent form may be computed by direct substitution (a tedious process), by matrix multiplication,[1] or by the use of explicit formulae. These latter relations are well known and may be found in Dickson's _Studies in the Theory of Numbers_.[2] The information contained in Lemma 1 below may be found there in slightly different notation and is stated here as a lemma for convenience in later reference to it.

LEMMA 1. _If_ (c_{jk}), $j,k = 1,2,3$, _is the matrix of a linear transformation of determinant_ $|c_{jk}| = 1$, _which takes_ f, _with coefficients_ $a_{ji} = a_{ij}$, _into the equivalent form_ f', _then the coefficients_ b_{sk}, $s,k = 1,2,3$, _of_ f' _are given by_

$$b_{sk} = X'_{1k}c_{1s} + X'_{2k}c_{2s} + X'_{3k}c_{3s}\ , \quad b_{ks} = b_{sk}\ , \tag{1}$$

---

[1] _Ibid._, p. 2.

[2] L.E. Dickson, _Studies in the Theory of Numbers_, (Chicago,) 1930, p. 5, (18) and (19).

and where

(2) $$X'_{ik} = a_{i1}c_{1k} + a_{i2}c_{2k} + a_{i3}c_{3k}\ , \quad i=1,2,3;$$

in particular,

(3) $$b_{kk} = f_k = f(c_{1k},\ c_{2k},\ c_{3k}).$$

PROOF. The coefficients b_{sk} of f' are given by

$$b_{sk} = \sum_{i,j=1}^{3} c_{is}a_{ij}c_{jk}\ , \quad j,k = 1,2,3.$$

Hence

$$b_{sk} = \sum_{i} c_{is} \sum_{j} a_{ij}c_{jk} = \sum_{i} c_{is}X'_{ik}\ ,$$

which is (1). Also, $b_{ks} = b_{sk}$.

The following result is due to E. H. Hadlock and is stated here without proof also for the purpose of later reference.[3]

LEMMA 2. *If* $f(x_1,\ x_2,\ x_3) = \sum_{i,j=1}^{3} a_{ij}x_ix_j,\ \ a_{ji} = a_{ij}$, *represents primitively* g *or* $-g$ *when* $x_j = x'_j$, $j = 1,2,3$, *where* g *is the g.c.d. of the values of the three linear functions*

---

[3] E. H. Hadlock, *Ternary Quadratic Forms Equivalent to Forms with One Term of Type* $2b_{ij}y_iy_j,\ j \neq i$ (Paper read at the four hundred ninety-sixth meeting of the American Mathematical Society, Spartanburg, S. C., November, 1953). Abstract published in Bulletin of the American Mathematical Society, Vol. 60, No. 1 (1954), p. 47.

(4) $$X_s' = a_{s1}x_1 + a_{s2}x_2 + a_{s3}x_3 \ , \quad s=1,2,3,$$

associated with f, when $x_j = x_j'$, then g is an arithmetical invariant of f with respect to any linear integral transformation of determinant one.

LEMMA 3. A necessary and sufficient condition that the form

$$f = \sum_{i,j=1}^{3} a_{ij}x_ix_j \ , \qquad a_{ji} = a_{ij} \ ,$$

of determinant $d \neq 0$ be equivalent to

$$f' = b_{11}y_1^2 + b_{22}y_2^2 + b_{33}y_3^2 + 2b_{12}y_1y_2 + 2Kb_{33}y_2y_3$$

is that f represent primitively g or $-g$, when $x_j = x_j'$, $j = 1, 2, 3$, where g is the g.c.d. of the values of the three linear functions

(4) $$X_s' = a_{s1}x_1 + a_{s2}x_2 + a_{s3}x_3 \ , \quad s=1,2,3,$$

associated with f, when $x_j = x_j'$, and where K is an arbitrary integer.

PROOF. Suppose that f is equivalent to f'. Then there exists a linear transformation (c_{jk}) with

(5) $$c_{12}C_{12} + c_{22}C_{22} + c_{32}C_{32} = 1$$

in which the set of cofactors C_{12}, C_{22}, C_{32} of c_{12}, c_{22}, c_{32} respectively is a primitive set. By Lemma 1, the coefficients

b_{sk} of f' are given by (1), where the X'_{ik}, $i = 1,2,3$, are defined by (2). The elements of the third column of (c_{jk}) are c_{13}, c_{23}, c_{33}, which comprise a primitive set. By (2),

$$X'_{13} = a_{11}c_{13} + a_{12}c_{23} + a_{13}c_{33}$$
$$X'_{23} = a_{12}c_{13} + a_{22}c_{23} + a_{23}c_{33}$$
$$X'_{33} = a_{13}c_{13} + a_{23}c_{23} + a_{33}c_{33} .$$

Not all of X'_{13}, X'_{23}, X'_{33} are equal to zero, for then $d = 0$, contrary to the hypothesis $d \neq 0$. Define X_{13}, X_{23}, and X_{33} by

(6) $$X'_{i3} = gX_{i3} , \qquad i = 1, 2, 3,$$

where

$$g = (X'_{13}, X'_{23}, X'_{33}).$$

All values, not all zero, of c_{11}, c_{21}, c_{31} for which

(7) $$X_{13}c_{11} + X_{23}c_{21} + X_{33}c_{31} = 0$$

are given by the second order determinants of the matrix

$$\begin{pmatrix} X_{13} & X_{23} & X_{33} \\ s & n & k \end{pmatrix},$$

namely,

(8) $$c_{11} = X_{23}k - X_{33}n$$
$$c_{21} = X_{33}s - X_{13}k$$
$$c_{31} = X_{13}n - X_{23}s ,$$

where the integral values of s, n, and k are chosen so that c_{11}, c_{21}, and c_{31} will be a primitive set. By (1), (6), and (7),

(9) $$b_{13} = g(X_{13}c_{11} + X_{23}c_{21} + X_{33}c_{31}) = 0$$

Since $f \sim f'$, not only must (9) hold, but also

(10) $$b_{23} = Kb_{33} .$$

Hence the system

(11) $$\begin{aligned} g(X_{13}c_{11} + X_{23}c_{21} + X_{33}c_{31}) &= 0 \\ g(X_{13}c_{12} + X_{23}c_{22} + X_{33}c_{32}) &= Kf(c_{13}, c_{23}, c_{33}) \end{aligned}$$

must be satisfied. By (3),

$$f(c_{13}, c_{23}, c_{33}) = b_{33} ,$$

by (1),

$$b_{33} = X'_{13}c_{13} + X'_{23}c_{23} + X'_{33}c_{33} ,$$

and by (6), g divides each of X'_{13}, X'_{23}, and X'_{33}. Hence g divides $f_3 = f(c_{13}, c_{23}, c_{33})$. Write

$$f_3 = gf_4 .$$

Then (11) becomes, upon division by g,

(12) $$\begin{aligned} X_{13}c_{11} + X_{23}c_{21} + X_{33}c_{31} &= 0 \\ X_{13}c_{12} + X_{23}c_{22} + X_{33}c_{32} &= Kf_4, \end{aligned}$$

a set of two independent equations, the first homogeneous and

the second non-homogeneous. The former has solutions, as shown by (8), and the second has integral solutions if and only if

$$(X_{13}, X_{23}, X_{33}) \mid Kf_4 ,$$

which is true since $(X_{13}, X_{23}, X_{33}) = 1$.

Let C_{jk} be the cofactor of c_{jk} in (c_{jk}). Then

(13)
$$\begin{aligned} C_{12} &= c_{31}c_{23} - c_{21}c_{33} \\ C_{22} &= c_{11}c_{33} - c_{31}c_{13} \\ C_{32} &= c_{21}c_{13} - c_{11}c_{23} \quad , \end{aligned}$$

which is, by (8),

(14)
$$\begin{aligned} C_{12} &= -(c_{23}X_{23} + c_{33}X_{33})s + c_{23}X_{13}n + c_{33}X_{13}k \\ C_{22} &= \ c_{13}X_{23}s - (c_{13}X_{13} + c_{33}X_{33})n + c_{33}X_{23}k \\ C_{32} &= \ c_{13}X_{33}s + c_{23}X_{33}n - (c_{13}X_{13} + c_{23}X_{23})k \ . \end{aligned}$$

By (5) and (14)

$$\begin{aligned} &c_{12}(-c_{23}X_{23}s - c_{33}X_{33}s + c_{23}X_{13}n + c_{33}X_{13}k) \\ &\quad + c_{22}(c_{13}X_{23}s - c_{13}X_{13}n - c_{33}X_{33}n + c_{33}X_{23}k) \\ &\qquad + c_{32}(c_{13}X_{33}s + c_{23}X_{33}n - c_{13}X_{13}k - c_{23}X_{23}k) = 1, \end{aligned}$$

or

(15)
$$\begin{aligned} &c_{13}s(c_{22}X_{23} + c_{32}X_{33}) + c_{23}n(c_{12}X_{13} + c_{32}X_{33}) \\ &+ c_{33}k(c_{12}X_{13} + c_{22}X_{23}) - c_{12}s(c_{23}X_{23} + c_{33}X_{33}) \\ &- c_{22}n(c_{13}X_{13} + c_{33}X_{33}) - c_{32}k(c_{13}X_{13} + c_{23}X_{23}) = 1 \ . \end{aligned}$$

From the second equation in (12) three substitutions are obtained, namely,

$$c_{22}X_{23} + c_{32}X_{33} = Kf_4 - c_{12}X_{13}$$
$$c_{12}X_{13} + c_{32}X_{33} = Kf_4 - c_{22}X_{23}$$
$$c_{12}X_{13} + c_{22}X_{23} = Kf_4 - c_{32}X_{33} ,$$

and these values, when placed in (15), give

$$\begin{aligned} &c_{13}s(Kf_4 - c_{12}X_{13}) + c_{23}n(Kf_4 - c_{22}X_{23}) \\ &+ c_{33}k(Kf_4 - c_{32}X_{33}) - c_{12}s(c_{23}X_{23} + c_{33}X_{33}) \\ &- c_{22}n(c_{13}X_{13} + c_{33}X_{33}) - c_{32}k(c_{13}X_{13} + c_{23}X_{23}) = 1, \end{aligned}$$

which when multiplied by -g becomes

$$(16) \qquad (c_{12}s + c_{22}n + c_{32}k)b_{33} - Kf_3(c_{13}s + c_{23}n + c_{33}k) = -g$$

After factoring (16) may be written as

$$(17) \qquad f_3\Big\{s(c_{12} - Kc_{13}) + n(c_{22} - Kc_{23}) + k(c_{32} - Kc_{33})\Big\} = -g.$$

Hence it is seen that f_3 must divide g. But from (2) and (6) it is known that g divides f_3. The first statement implies that $|f_3| \leq g$, and the second, that $g \leq |f_3|$. Hence $|f_3| = g$, which is to say that f represents primitively, when $x_j = x_j' \equiv c_{j3}$, g or -g, where g is the g.c.d. of the values of the three functions X_s' as defined in (4), when $x_j = x_j'$.

The condition is sufficient, for s, n, and k are arbitrary; so let s, n, k be a primitive set; then (17) is

satisfied, i.e., there exist integers $c_{i2} - Kc_{i3}$, $i=1,2,3$, satisfying (17), since the g.c.d. of the three s, n, and k divides $-g/f_3 = 1$ or -1. Relation (16), upon division by g, yields, by (6), (15), which retraces to (5). The values s, n, and k are placed in (8) to produce values of the c_{11}, c_{21}, and c_{31} satisfying (7). From (5), $|c_{jk}| = 1$. From (12), $b_{23} = Kb_{33}$, and (7) implies that $b_{13} = 0$. These are the explicit properties of f'; hence $f \sim f'$. Moreover (5) may be rewritten as

$$c_{11}C_{11} + c_{21}C_{21} + c_{31}C_{31} = 1,$$

and it may therefore be seen that $(c_{11}, c_{21}, c_{31}) = 1$. This completes the proof of Lemma 3.

COROLLARY 1. If the form

$$f = \sum_{i,j=1}^{3} a_{ij}x_i x_j , \qquad a_{ji} = a_{ij} ,$$

of determinant $d \neq 0$ represents one, then f is equivalent to

$$f' = b_{11}y_1^2 + b_{22}y_2^2 + b_{33}y_3^2 + 2b_{12}y_1y_2 + 2Kb_{33}y_2y_3.$$

COROLLARY 2. A necessary and sufficient condition that the form

$$f = \sum_{i,j=1}^{3} a_{ij}x_i x_j , \qquad a_{ji} = a_{ij} ,$$

<u>of determinant</u> $d \neq 0$ <u>be equivalent to</u>

$$f' = b_{11}y_1^2 + b_{22}y_2^2 + b_{33}y_3^2 + 2b_{12}y_1y_2$$

<u>is that</u> f <u>represent primitively</u> g <u>or</u> $-g$, <u>when</u> $x_j = x_j'$, $j = 1,2,3$, <u>where</u> g <u>is the g.c.d. of the values of the three linear functions (4) associated with</u> f <u>when</u> $x_j = x_j'$.

This Corollary is a special case of, and follows directly from, Lemma 3. However, it has been proved independently by E. H. Hadlock.[4]

COROLLARY 3. <u>A necessary condition that the form</u>

$$f = \sum_{i,j=1}^{3} a_{ij}x_ix_j, \qquad a_{ji} = a_{ij},$$

<u>of determinant</u> $d \neq 0$ <u>be equivalent to the form</u>

$$f' = b_{11}y_1^2 + b_{22}y_2^2 + b_{33}y_3^2 + 2b_{12}y_1y_2 + 2Kb_{33}y_2y_3$$

<u>is that</u> $g = |b_{33}|$, <u>where</u> g <u>is the g.c.d. of the values of the three linear functions</u> X_s' <u>defined by (4)</u>.

PROOF. By Lemma 3, $f_3 = \pm g$. By (3), $b_{33} = f_3$. Hence $b_{33} = \pm g$. But since g is a g.c.d., g must be positive. Therefore, $g = |b_{33}|$.

This Corollary is applicable to the special case of $K = 0$, and for this case the reader is referred to the remark which

---

[4] <u>Ibid.</u>

follows Corollary 2.

Corollary 4 below concerns a very special type of form, a form having but one cross-product. Although this is a highly restricted type of form, its occurrence is frequent; many forms of this type may be found in a table of reduced forms.[5] Moreover, in the next chapter it will be shown that such forms exist for every value of determinant $d \neq 0$.

COROLLARY 4. <u>If the form</u>

$$f = a_{11}x_1{}^2 + a_{22}x_2{}^2 + a_{33}x_3{}^2 + 2a_{23}x_2x_3$$

<u>of determinant</u> $d \neq 0$ <u>is equivalent to the form</u>

$$f' = b_{11}y_1{}^2 + b_{22}y_2{}^2 + b_{33}y_3{}^2 + 2b_{12}y_1y_2 \ ,$$

<u>and if</u> (c_{jk}) <u>is the matrix of the transformation of determinant one which sends</u> f <u>into</u> f', <u>then</u> b_{33} <u>divides</u> $a_{11}c_{13}$; <u>in particular, if</u> $a_{11} = \pm 1$, <u>then</u> c_{13} <u>is a multiple of</u> b_{33}.

PROOF: By (2), $X'_{13} = a_{11}c_{13}$; also, g divides X'_{i3}, $i=1,2,3$. Further, from Corollary 3, $g = |b_{33}|$. Hence $b_{33} \mid a_{11}c_{13}$.

THEOREM 1. <u>A necessary condition that the form</u>

$$f = \sum_{i,j=1}^{3} a_{ij}x_ix_j \ , \qquad a_{ji} = a_{ij} \ ,$$

---

[5] L. E. Dickson, <u>Studies in the Theory of Numbers</u>, pp. 150-151; 181-185.

of determinant $d \neq 0$ be equivalent to

$$f' = b_{11}y_1^2 + b_{22}y_2^2 + b_{33}y_3^2 + 2b_{12}y_1y_2 + 2Kb_{33}y_2y_3 ,$$

K any integer, is that f represent primitively, when $x_j = x_j'$, a divisor of d.

PROOF. Since by Theorem 4 of Dickson's Studies in the Theory of Numbers equivalent (n-ary) forms have the same determinant,[6] then

$$d = \begin{vmatrix} b_{11} & b_{12} & 0 \\ b_{12} & b_{22} & Kb_{33} \\ 0 & Kb_{33} & b_{33} \end{vmatrix},$$

which may be factored as

$$d = b_{33} \begin{vmatrix} b_{11} & b_{12} & 0 \\ b_{12} & b_{22} & K \\ 0 & Kb_{33} & 1 \end{vmatrix} .$$

But by (3),

$$b_{33} = f_3 .$$

Hence f_3 divides d, the determinant of the form f.

In order that the general ternary form f with unrestricted coefficients a_{ij} be equivalent to f', certain necessary conditions must be met. Further, given certain suf-

---

[6] Ibid., p. 7.

ficient conditions, f will be equivalent to f'. Thus there are a number of necessary and/or sufficient conditions that f and f' be equivalent. These conditions evidently depend upon the values of the coefficients of the form f'. Hence if f' is a highly restricted type of form, then the conditions for equivalence of f and f' will be quite stringent; reciprocally, if the form f' is not so highly restricted, then the conditions for equivalence of f and f' will be less rigid. It should be noted that conditions for equivalence are usually expressed in terms of whether the given form f represents (or represents primitively) one or more integers.

Given any two forms f and f', one obviously necessary condition for equivalence is that their determinants be equal. Other necessary conditions might be written similarly for other arithmetic invariants, e.g., τ and σ . Clearly such conditions are not sufficient for equivalence.

An interesting necessary condition that the general form

$$f = \sum_{i,j=1}^{3} a_{ij}x_ix_j , \qquad a_{ji} = a_{ij} ,$$

be equivalent to the form

$$f' = Ay_1^2 + b_{22}y_2^2 + b_{33}y_3^2 + 2b_{12}y_1y_2 + 2b_{13}y_1y_3 + 2b_{23}y_2y_3,$$

where A is any integer, is that f represent A primitively. The proof of this follows directly from (3). For since $f \sim f'$, then by Lemma 1, $f(c_{11}, c_{21}, c_{31}) = b_{11} = A$, and the c_{i1},

$i = 1, 2, 3$, constitute a primitive set, so that f represents A primitively. The converse of the statement holds, that if f represents A primitively, then f is equivalent to a form having A as the coefficient of y_1^2, and this converse is proved and stated as a theorem in Dickson's Studies in the Theory of Numbers.[7] Similar statements hold for equivalence to a form having A as the coefficient of y_2^2 or y_3^2, as evidenced by the three separate statements given in (3).

The form f' of Theorem 2 below is the particular f' form of Lemma 3, Corollaries 1 and 3, and Theorem 1. Conditions for equivalence of f and f' which were stated in those propositions pertained principally to representation of some integer by the form f. The next condition relates to the adjoint of f.

THEOREM 2. *A necessary and sufficient condition for the equivalence of the forms*

$$f = \sum_{i,j=1}^{3} a_{ij}x_i x_j , \qquad a_{ji} = a_{ij} ,$$

of determinant $d \neq 0$, *and*

$$f' = b_{11}y_1^2 + b_{22}y_2^2 + b_{33}y_3^2 + 2b_{12}y_1y_2 + 2Kb_{33}y_2y_3$$

---

[7] Ibid., p. 12, Theorem 10.

<u>is that</u> $g\phi(X_{13},X_{23},X_{33})$ <u>be equal to</u> d <u>or</u> -d, <u>where</u> g <u>is the g.c.d. of the values of the three linear functions</u> X_s' <u>associated with</u> f, <u>when</u> $x_j = x_j'$, <u>and the</u> X_{i3}, $i = 1,2,3$, <u>are defined by (6), and where</u> ϕ <u>is the adjoint of</u> f.

PROOF. To prove the condition necessary, take as hypothesis that $f \sim f'$. Then by Lemma 3, f must represent, when $x_j = x_j' \equiv c_{j3}$, either g or -g, where g is the g.c.d. of the values of the three linear functions X_s', $s = 1,2,3$, associated with f, when $x_j = x_j'$. The double sign ($\pm$) in relation (18) is to be taken as either positive or negative, not necessarily both.

$$f_3 = \pm g \tag{18}$$

Multiplication of both members of (18) by d^2 gives

$$\pm d^2 g = d^2 f(c_{13},c_{23},c_{33})$$

and

$$\pm d^2 g = f(dc_{13},dc_{23},dc_{33}). \tag{19}$$

By (2) and (6) there exists a set of values c_{13}, c_{23}, c_{33} with $(c_{13}, c_{23}, c_{33}) = 1$ of x_1, x_2, x_3 such that

$$\begin{aligned} X_{13}' &= a_{11}c_{13} + a_{12}c_{23} + a_{13}c_{33} = X_{13}g \\ X_{23}' &= a_{12}c_{13} + a_{22}c_{23} + a_{23}c_{33} = X_{23}g \\ X_{33}' &= a_{13}c_{13} + a_{23}c_{23} + a_{33}c_{33} = X_{33}g \, , \end{aligned}$$

where $(X_{13}, X_{23}, X_{33}) = 1$. Solving the above set of equations for dc_{13}, dc_{23}, and dc_{33}, one obtains

(20) $$\begin{aligned} dc_{13} &= gN_1 \\ dc_{23} &= gN_2 \\ dc_{33} &= gN_3 , \end{aligned}$$

where

(21) $$\begin{aligned} N_1 &= A_{11}X_{13} + A_{12}X_{23} + A_{13}X_{33} \\ N_2 &= A_{12}X_{13} + A_{22}X_{23} + A_{23}X_{33} \\ N_3 &= A_{13}X_{13} + A_{23}X_{23} + A_{33}X_{33} , \end{aligned}$$

and where the A_{ij} are the cofactors of the elements a_{ij} of d. Substitution of (20) into (19) gives

$$\pm\, d^2 g = f(gN_1, gN_2, gN_3) ,$$

$$\pm\, d^2 g = g^2 f(N_1, N_2, N_3) ,$$

or

(22) $$\pm\; d^2 = gf(N_1, N_2, N_3) .$$

By (4), which is

$$X_s' = a_{s1}x_1 + a_{s2}x_2 + a_{s3}x_3 , \quad s = 1,2,3,$$

use as index the letter i rather than s so that

$$X_i' = a_{i1}x_1 + a_{i2}x_2 + a_{i3}x_3 , \quad i = 1,2,3.$$

Then

$$f(N_1, N_2, N_3) = X_1'N_1 + X_2'N_2 + X_3'N_3 ,$$

$$X_i' = X_i'(N_1, N_2, N_3),\ i = 1,2,3.$$

By (21)

$$X_i'(N_1, N_2, N_3) = dX_{i3} .$$

Therefore, by (21),

$$f(N_1, N_2, N_3) = dX_{13}N_1 + dX_{23}N_2 + dX_{33}N_3$$

or

$$f(N_1, N_2, N_3) = d\phi(X_{13}, X_{23}, X_{33}) \tag{23}$$

where $\phi(x_1,x_2,x_3)$ is the adjoint form of the form

$$f(x_1,x_2,x_3) = \sum_{i,j=1}^{3} a_{ij}x_ix_j, \qquad a_{ji} = a_{ij} .$$

Substitution of (23) into (22) gives

$$\pm d^2 = gd\phi(X_{13}, X_{23}, X_{33})$$

or

$$\pm d = g\phi(X_{13}, X_{23}, X_{33}) . \tag{24}$$

The relation (24) states that $g\phi(X_{13}, X_{23}, X_{33})$ equals the determinant of f or its negative, which was to be proved.

The sufficient condition follows readily by retracing the steps (18) to (24). Then since (18) holds, application of Lemma 3 guarantees that $f \sim f'$. This completes the proof of Theorem 2.

Throughout this chapter conditions were sought that a general form f be equivalent to a form f' of a specified type. Several conditions were obtained; some of these are useful in particular applications, while others are rather unwieldy. In the practice of determining whether two forms are equivalent one must, since the specific transformation is not known, resort to all possible means for testing equivalence. It will be shown that certain of the conditions for equivalence developed in this chapter do serve in some cases as useful tests for equivalence.

Examples

Several representative examples are given here to illustrate the preceding results. Consider the form

$$f = -37x_1^2 + 9x_2^2 + 3x_3^2 - 30x_1x_2 + 52x_1x_3 + 56x_2x_3$$

of determinant $d = -590$. One may apply to f the transformation

$$T: \quad \begin{aligned} x_1 &= y_1 - y_2 - y_3 \\ x_2 &= -y_1 + 2y_2 + y_3 \\ x_3 &= y_1 - y_2 \end{aligned} \quad ,$$

whose matrix is written

$$(c_{jk}) = \begin{pmatrix} 1 & -1 & -1 \\ -1 & 2 & 1 \\ 1 & -1 & 0 \end{pmatrix},$$

and which is of determinant one, to obtain an equivalent form f'. First Lemma 1 will be applied in order to obtain the coefficients b_{sk} of f' explicitly. By (2),

$$X'_{11} = (-37)(1) + (-15)(-1) + (26)(1) = 4$$
$$X'_{21} = (-15)(1) + (9)(-1) + (28)(1) = 4$$
$$X'_{31} = (26)(1) + (28)(-1) + (3)(1) = 1$$
$$X'_{12} = (-37)(-1) + (-15)(2) + (26)(-1) = -19$$
$$X'_{22} = (-15)(-1) + (9)(2) + (28)(-1) = 5$$
$$X'_{32} = (26)(-1) + (28)(2) + (3)(-1) = 27$$
$$X'_{13} = (-37)(-1) + (-15)(1) + (26)(0) = 22$$
$$X'_{23} = (-15)(-1) + (9)(1) + (28)(0) = 24$$
$$X'_{33} = (26)(-1) + (28)(1) + (3)(0) = 2 .$$

Placing these values in (1),

$$b_{11} = (4)(1) + (4)(-1) + (1)(1) = 1$$
$$b_{12} = (-19)(1) + (5)(-1) + (27)(1) = 3$$
$$b_{13} = (22)(1) + (24)(-1) + (2)(1) = 0$$
$$b_{22} = (-19)(-1) + (5)(2) + (27)(-1) = 2$$
$$b_{23} = (22)(-1) + (24)(2) + (2)(-1) = 24$$
$$b_{33} = (22)(-1) + (24)(1) + (2)(0) = 2 .$$

Also, by (3),

$$b_{11} = f(1,-1,1) = 1,$$
$$b_{22} = f(-1,2,-1) = 2,$$
and $b_{33} = f(-1,1,0) = 2.$

Thus the form f' may be written

$$f' = y_1^2 + 2y_2^2 + 2y_3^2 + 6y_1y_2 + 48y_2y_3 .$$

The form f' just obtained may be considered as the f' of some of the preceding propositions, namely, Lemma 3, Corollaries 1 and 3, and Theorems 1 and 2, for $b_{23} = Kb_{33}$, or $24 = 2K$, so that $K = 12$. By Lemma 3, a necessary and sufficient condition that $f \sim f'$ is that f_3 equal g or $-g$. Since $f_3 = 2$ and $g = 2$, this condition is satisfied.

Corollary 3 is illustrated in that $g = |b_{33}| = |2| = 2$. By Theorem 2 $g\phi(X_{13}, X_{23}, X_{33})$ must equal d or $-d$. The adjoint of the form f is computed and is found to be

$$\phi(x_1, x_2, x_3) = -757x_1^2 - 787x_2^2 - 558x_3^2 + 1546x_1x_2 - 1308x_1x_3 + 1292x_2x_3 .$$

By (6), the values of X_{13}, X_{23}, and X_{33} are found to be 11, 12, and 1 respectively.

Then

$$\phi(11, 12, 1) = -91597 - 113328 - 558 + 204072 - 14388 + 15504 = -295.$$

Hence

$$g\phi(X_{13}, X_{23}, X_{33}) = 2(-295) = -590.$$

Since $g\phi(X_{13}, X_{23}, X_{33}) = -590 = d$, the condition of Theorem 2 is satisfied.

Theorem 1 is illustrated by the form

$$f = -18x_1^2 + 7x_2^2 + 6x_3^2 - 16x_1x_2 + 26x_1x_3 + 36x_2x_3$$

and the equivalent form

$$f' = y_1^2 + 2y_2^2 + 5y_3^2 + 2y_1y_2 + 30y_2y_3$$

which is obtained by subjecting the form f to the transformation T of determinant one. By Theorem 1, f_3 must divide d. By computation, $f_3 = f(-1, 1, 0) = 5$. Since 5 divides $d = -235$, the theorem is illustrated.

CHAPTER III

CONSTRUCTION OF A FORM f EQUIVALENT TO SOME FORM f' WITH $b_{13} = b_{23} = 0$

In the preceding chapter the form

$$f' = b_{11}y_1^2 + b_{22}y_2^2 + b_{33}y_3^2 + 2b_{12}y_1y_2 + 2Kb_{33}y_2y_3$$

was considered. A special case of f' occurs when $K = 0$. By Corollary 3 a necessary condition that a form

$$f = \sum_{i,j=1}^{3} a_{ij}x_ix_j, \qquad a_{ji} = a_{ij} ,$$

of determinant $d \neq 0$, be equivalent to a form f' with $K = 0$ is that $g = |b_{33}|$. In order to exhibit this property one should have a method of obtaining a form f which will be equivalent to f'. It might be wondered whether such forms exist for every value d for determinant. In this chapter this last question is answered affirmatively, and an explicit method for constructing such forms of determinant d, where d is any non-zero integer, is given.

Consider the form

$$f' = b_{11}y_1^2 + b_{22}y_2^2 + b_{33}y_3^2 + 2b_{12}y_1y_2 .$$

All such forms f' are classified into three mutually exclusive types: type A, any form f' with $b_{11} = b_{12}$; type B, a form f' with $b_{11} \neq b_{12}$ and $(b_{11}, b_{12}) = 1$; and type C, a form f' with $b_{11} \neq b_{12}$ and $(b_{11}, b_{12}) = b > 1$. The construction of a form f equivalent to f' will be accomplished separately for the three different types of f'.

Type A: $b_{11} = b_{12}$

Given any integer $d \neq 0$ and a form f' of type A, if such exists, of determinant d, then application of any unimodular transformation will yield a form f equivalent to f'. Since determinants of equivalent forms are equal, then the value d of the determinant of f is given as follows:

$$d = \begin{vmatrix} b_{11} & b_{12} & 0 \\ b_{12} & b_{22} & 0 \\ 0 & 0 & b_{33} \end{vmatrix} = b_{33}(b_{11}b_{22} - b_{12}^2) .$$

Since $b_{11} = b_{12}$, then $d = b_{33}b_{11}(b_{22} - b_{11})$.

Given any integer $d \neq 0$, factor d into two factors, not necessarily prime or relatively prime,

$$d = b_{33}b_{11} .$$

Assign to b_{22} the value $b_{22} = b_{11} + 1$. Then a form f' having such coefficients is of determinant

$$\begin{vmatrix} b_{11} & b_{11} & 0 \\ b_{11} & b_{11}+1 & 0 \\ 0 & 0 & b_{33} \end{vmatrix} = b_{33}\left[(b_{11}+1)b_{11}-b_{11}^{2}\right] = b_{33}b_{11} = d.$$

Let c_{11}, c_{21}, c_{31} and C_{13}, C_{23}, C_{33} be two primitive sets such that

$$c_{11}C_{13} + c_{21}C_{23} + c_{31}C_{33} = 0.$$

Then there exists a primitive set c_{12}, c_{22}, c_{32} for which

$$C_{13} = c_{21}c_{32} - c_{31}c_{22}$$
$$C_{23} = c_{31}c_{12} - c_{11}c_{32}$$
$$C_{33} = c_{11}c_{22} - c_{21}c_{12} ,$$

by Theorem 9 of Dickson's <u>Studies in the Theory of Numbers</u>.[1] Let c_{13}, c_{23}, c_{33} be any three integers satisfying

$$c_{13}C_{13} + c_{23}C_{23} + c_{33}C_{33} = 1.$$

Then the matrix (c_{jk}), $j,k = 1,2,3$, represents the matrix of a linear transformation of determinant one. Consider the transformation (c'_{jk}) which is the inverse transformation of (c_{jk}). The inverse transformation is given by

---

[1] <u>Ibid</u>., p. 11.

$$(25)\qquad (c'_{jk}) \equiv \begin{pmatrix} c_{22}c_{33}-c_{23}c_{32} & c_{13}c_{32}-c_{12}c_{33} & c_{12}c_{23}-c_{13}c_{22} \\ c_{23}c_{31}-c_{21}c_{33} & c_{11}c_{33}-c_{31}c_{13} & c_{13}c_{21}-c_{11}c_{23} \\ c_{21}c_{32}-c_{22}c_{31} & c_{12}c_{31}-c_{11}c_{32} & c_{11}c_{22}-c_{21}c_{12} \end{pmatrix}.$$

If the transformation (c'_{jk}) is applied to the form

$$f' = b_{11}y_1^{\,2} + b_{22}y_2^{\,2} + b_{33}y_3^{\,2} + 2b_{11}y_1y_2 \,,$$

then f' is carried into some equivalent form

$$f = \sum_{i,j=1}^{3} a_{ij}x_ix_j, \qquad a_{ji} = a_{ij} \,.$$

Thus there exists a form f, as given above, which is carried into f' by the transformation (c_{jk}).

Define Y'_{ik} similarly to the X'_{ik} given in (2) by

$$(26)\qquad Y'_{ik} = b_{i1}c'_{1k} + b_{i2}c'_{2k} + b_{i3}c'_{3k} \quad , \; i = 1,2,3.$$

Then by Lemma 1, if the transformation (c'_{jk}) is applied to the form f', the coefficients a_{sk} of the equivalent form f are given by

$$(27)\qquad a_{sk} = Y'_{1k}c'_{1s} + Y'_{2k}c'_{2s} + Y'_{3k}c'_{3s} \,.$$

Applying relations (25) and (26) to the particular form f' with $b_{12} = b_{11}$, $b_{22} = b_{11} + 1$ gives

$$Y'_{11} = b_{11}c_{22}c_{33} - b_{11}c_{23}c_{32} + b_{11}c_{23}c_{31} - b_{11}c_{21}c_{33}$$

$$\begin{aligned} Y'_{21} = b_{11}c_{22}c_{33} - b_{11}c_{23}c_{32} + b_{11}c_{23}c_{31} \\ - b_{11}c_{21}c_{33} + c_{23}c_{31} - c_{21}c_{33} \end{aligned}$$

$$Y'_{31} = b_{33}c_{21}c_{32} - b_{33}c_{22}c_{31}$$
$$Y'_{12} = b_{11}c_{13}c_{32} - b_{11}c_{12}c_{33} + b_{11}c_{11}c_{33} - b_{11}c_{31}c_{13}$$
$$Y'_{22} = b_{11}c_{13}c_{32} - b_{11}c_{12}c_{33} + b_{11}c_{11}c_{33}$$
$$- b_{11}c_{31}c_{13} + c_{11}c_{33} - c_{31}c_{13}$$
$$Y'_{32} = b_{33}c_{12}c_{31} - b_{33}c_{11}c_{32}$$
$$Y'_{13} = b_{11}c_{12}c_{23} - b_{11}c_{13}c_{22} + b_{11}c_{13}c_{21} - b_{11}c_{11}c_{23}$$
$$Y'_{23} = b_{11}c_{12}c_{23} - b_{11}c_{13}c_{22} + b_{11}c_{13}c_{21}$$
$$- b_{11}c_{11}c_{23} + c_{13}c_{21} - c_{11}c_{23}$$
$$Y'_{33} = b_{33}c_{11}c_{22} - b_{33}c_{12}c_{21} .$$

By (27) the first coefficient a_{11} of the form f is computed.

$$a_{11} = (b_{11}c_{22}c_{33} - b_{11}c_{23}c_{32} + b_{11}c_{23}c_{31} - b_{11}c_{21}c_{33})(c_{22}c_{33}$$
$$- c_{23}c_{32}) + (b_{11}c_{22}c_{33} - b_{11}c_{23}c_{32} + b_{11}c_{23}c_{31}$$
$$- b_{11}c_{21}c_{33} + c_{23}c_{31} - c_{21}c_{33})(c_{23}c_{31} - c_{21}c_{33})$$
$$+ (b_{33}c_{21}c_{32} - b_{33}c_{22}c_{31})(c_{21}c_{32} - c_{22}c_{31}).$$

Carrying out all indicated multiplications,

$$a_{11} = b_{11}c_{22}^2c_{33}^2 - b_{11}c_{22}c_{23}c_{32}c_{33} + b_{11}c_{22}c_{23}c_{31}c_{33}$$
$$- b_{11}c_{21}c_{22}c_{33}^2 - b_{11}c_{22}c_{23}c_{32}c_{33} + b_{11}c_{23}^2c_{32}^2$$
$$- b_{11}c_{23}^2c_{31}c_{32} + b_{11}c_{21}c_{23}c_{32}c_{33} + b_{11}c_{22}c_{23}c_{31}c_{33}$$
$$- b_{11}c_{23}^2c_{31}c_{32} + b_{11}c_{23}^2c_{31}^2 - b_{11}c_{21}c_{23}c_{31}c_{33}$$
$$+ c_{23}^2c_{31}^2 - c_{21}c_{23}c_{31}c_{33} - b_{11}c_{21}c_{22}c_{33}^2$$
$$+ b_{11}c_{21}c_{23}c_{32}c_{33} - b_{11}c_{21}c_{23}c_{31}c_{33} + b_{11}c_{21}^2c_{33}^2$$

$$- c_{21}c_{23}c_{31}c_{33} + c_{21}^2c_{33}^2 + b_{33}c_{21}^2c_{32}^2$$
$$- b_{33}c_{21}c_{22}c_{31}c_{32} - b_{33}c_{21}c_{22}c_{31}c_{32} + b_{33}c_{22}^2c_{31}^2 .$$

Upon collection of like terms this reduces to

$$\begin{aligned} a_{11} = {} & b_{11}c_{22}^2c_{33}^2 + b_{11}c_{23}^2c_{32}^2 + b_{11}c_{21}^2c_{33}^2 + b_{33}c_{21}^2c_{32}^2 \\ & + b_{33}c_{22}^2c_{31}^2 + b_{11}c_{23}^2c_{31}^2 - 2b_{11}c_{22}c_{23}c_{32}c_{33} \\ & + 2b_{11}c_{22}c_{23}c_{31}c_{33} + 2b_{11}c_{21}c_{23}c_{32}c_{33} - 2b_{11}c_{21}c_{23}c_{31}c_{33} \\ & - 2b_{33}c_{21}c_{22}c_{31}c_{32} - 2b_{11}c_{21}c_{22}c_{33}^2 - 2b_{11}c_{23}^2c_{31}c_{32} \\ & -2c_{21}c_{23}c_{31}c_{33} + c_{23}^2c_{31}^2 + c_{21}^2c_{33}^2 . \end{aligned}$$

After appropriate factoring, one obtains

$$\begin{aligned} a_{11} = {} & (c_{31}c_{23} - c_{21}c_{33})^2 + b_{11}(c_{22}c_{33} - c_{23}c_{32})^2 \\ & + b_{11}(c_{23}c_{31} - c_{21}c_{33})^2 + b_{33}(c_{21}c_{32} - c_{22}c_{31})^2 \\ & + 2b_{11}(c_{22}c_{33} - c_{23}c_{32})(c_{23}c_{31} - c_{21}c_{33}). \end{aligned}$$

Now denote by C_{jk} the cofactor of the element c_{jk} in (c_{jk}). Then the above equation may be written as

$$a_{11} = C_{12}^2 + b_{11}(C_{11} + C_{12})^2 + b_{33}C_{13}^2 . \tag{28}$$

In the same manner each a_{ij}, $i,j = 1,2,3$, may be computed. The result of this computation is as follows:

$$\begin{aligned} a_{11} &= C_{12}^2 + b_{11}(C_{11} + C_{12})^2 + b_{33}C_{13}^2 \\ a_{22} &= C_{22}^2 + b_{11}(C_{21} + C_{22})^2 + b_{33}C_{23}^2 \\ a_{33} &= C_{32}^2 + b_{11}(C_{31} + C_{32})^2 + b_{33}C_{33}^2 \end{aligned}$$

$$a_{12} = C_{12}C_{22} + b_{11}(C_{11} + C_{12})(C_{21} + C_{22}) + b_{33}C_{13}C_{23}$$
$$a_{13} = C_{12}C_{32} + b_{11}(C_{11} + C_{12})(C_{31} + C_{32}) + b_{33}C_{13}C_{33}$$
$$a_{23} = C_{22}C_{32} + b_{11}(C_{21} + C_{22})(C_{31} + C_{32}) + b_{33}C_{23}C_{33} .$$

The foregoing discussion provides a method by which, given any integer $d \neq 0$, a form f of determinant d may be constructed which is equivalent to some form f' of type A.

THEOREM 3. Given any integer $d \neq 0$, there exists a form

$$f' = b_{11}y_1^2 + b_{22}y_2^2 + b_{33}y_3^2 + 2b_{11}y_1y_2$$

of determinant $d = b_{11}b_{33}$. The coefficients of a form f equivalent to f' are given by

$$(29) \qquad a_{ij} = C_{i2}C_{j2} + b_{11}(C_{i1} + C_{i2})(C_{j1} + C_{j2}) + b_{33}C_{i3}C_{j3},$$

and in particular

$$(30) \qquad a_{ii} = C_{i2}^2 + b_{11}(C_{i1} + C_{i2})^2 + b_{33}C_{i3}^2,$$

where the C_{ij} are cofactors of the elements of any matrix (c_{jk}) of determinant one.

Evidently such a form f as obtained by the use of the above method must satisfy the results of Corollary 3, i.e., it must be true that $g = |b_{33}|$. To demonstrate this compute the three X'_{i3} by (2).

$$X'_{13} = a_{11}c_{13} + a_{12}c_{23} + a_{13}c_{33}$$

$$\begin{aligned} X'_{13} = {} & c_{13}\left[C_{12}{}^2 + b_{11}(C_{11} + C_{12})^2 + b_{33}C_{13}{}^2\right] \\ & + c_{23}\left[C_{12}C_{22} + b_{11}(C_{11} + C_{12})(C_{21} + C_{22}) \right. \\ & \left. + b_{33}C_{13}C_{23}\right] + c_{33}\left[C_{12}C_{32} + b_{11}(C_{11} \right. \\ & \left. + C_{12})(C_{31} + C_{32}) + b_{33}C_{13}C_{33}\right] \end{aligned}$$

$$\begin{aligned} X'_{13} = {} & C_{12}(c_{13}C_{12} + c_{23}C_{22} + c_{33}C_{32}) \\ & + b_{11}C_{11}(c_{13}C_{11} + c_{23}C_{21} + c_{33}C_{31}) \\ & + b_{11}C_{11}(c_{13}C_{12} + c_{23}C_{22} + c_{33}C_{32}) \\ & + b_{11}C_{12}(c_{13}C_{11} + c_{23}C_{21} + c_{33}C_{31}) \\ & + b_{11}C_{12}(c_{13}C_{12} + c_{23}C_{22} + c_{33}C_{32}) \\ & + b_{33}C_{13}(c_{13}C_{13} + c_{23}C_{23} + c_{33}C_{33}) \end{aligned}$$

Since $c_{13}C_{1s} + c_{23}C_{2s} + c_{33}C_{3s}$ equals 1 for $s = 3$ and 0 for $s = 1$ or $s = 2$, the above equation may be written as

$$X'_{13} = b_{33}C_{13} .$$

Similarly, $X'_{23} = b_{33}C_{23}$ and $X'_{33} = b_{33}C_{33}$. Since $c_{13}C_{13} + c_{23}C_{23} + c_{33}C_{33} = 1$, then $(C_{13}, C_{23}, C_{33}) = 1$. Therefore

$$\begin{aligned} g = (X'_{13}, X'_{23}, X'_{33}) &= (b_{33}C_{13}, b_{33}C_{23}, b_{33}C_{33}) \\ &= (b_{33}, b_{33}, b_{33}) = |b_{33}|, \text{ as expected.} \end{aligned}$$

This completes the discussion of the constructed form of type A.

Type B: $b_{11} \neq b_{12}$, $(b_{11}, b_{12}) = 1$

Consider a form f' of type B. Any form f equivalent to f' is of determinant

$$d = \begin{vmatrix} b_{11} & b_{12} & 0 \\ b_{12} & b_{22} & 0 \\ 0 & 0 & b_{33} \end{vmatrix} = b_{33}B_{33} .$$

Thus b_{33} divides d and $B_{33} = d/b_{33}$. For any given integer $d \neq 0$, write $d = b_{33}B_{33}$ so that B_{33} is positive. Then b_{33} is positive or negative according as d is positive or negative. Now

(31) $$B_{33} = b_{11}b_{22} - b_{12}^2$$

may be written as the congruence

(32) $$b_{12}^2 \equiv -B_{33} \pmod{b_{11}}$$

If congruence (32) is solvable in integers, then it must be true that

(33) $$\left(\frac{-B_{33}}{b_{11}}\right) = +1 .$$

Then by the quadratic reciprocity law,

(34) $$\left(\frac{b_{11}}{B_{33}}\right) = (-1)^{\frac{B_{33}+1}{2}\,\frac{b_{11}-1}{2}}$$

Therefore, given any integer $d \neq 0$, let B_{33} be any odd prime factor of d. Then by relation (34) and Dirichlet's Theorem, obtain an odd prime b_{11}. In case d contains no odd prime as a factor, let $B_{33} = 1$ and by (33) obtain an odd prime b_{11}. This guarantees the existence of an integer b_{12} satisfying (32). Then b_{22}, as defined by (31), will be an integer. Finally $b_{33} = d/B_{33}$. Hence the coefficients have been obtained for some form

$$f' = b_{11}y_1^2 + b_{22}y_2^2 + b_{33}y_3^2 + 2b_{12}y_1y_2$$

of type B and of a given determinant $d = b_{33}B_{33} \neq 0$.

In the same manner as in the discussion of the construction of a form of type A, let c_{11}, c_{21}, c_{31} and c_{12}, c_{22}, c_{32} be any two primitive sets such that the g.c.d. of the cofactors C_{13}, C_{23}, and C_{33} is one. Choose c_{13}, c_{23}, and c_{33} to be any three integers satisfying

$$c_{13}C_{13} + c_{23}C_{23} + c_{33}C_{33} = 1.$$

Then (c_{jk}) is the matrix of a linear unimodular transformation. The inverse transformation (c'_{jk}) sending f' into some form f is given by

$$(c'_{jk}) \equiv \begin{pmatrix} C_{11} & C_{21} & C_{31} \\ C_{12} & C_{22} & C_{32} \\ C_{13} & C_{23} & C_{33} \end{pmatrix}.$$

Since $c'_{jk} = C_{kj}$, where C_{jk} is the cofactor of c_{jk} in (c_{jk}), the relations (35) and (36) of type B, which correspond to relations (26) and (27) of type A are given by

$$Y'_{ik} = b_{i1}C_{k1} + b_{i2}C_{k2} + b_{i3}C_{k3} \tag{35}$$

and

$$a_{sk} = Y'_{1k}C_{s1} + Y'_{2k}C_{s2} + Y'_{3k}C_{s3}\,. \tag{36}$$

The a_{sk} are, by Lemma 1, the coefficients of a form f equivalent to f'. Computation of the values of the nine Y'_{ik} results in

$$\begin{aligned}
Y'_{11} &= b_{11}C_{11} + b_{12}C_{12} & \qquad Y'_{31} &= b_{33}C_{13}\\
Y'_{12} &= b_{11}C_{21} + b_{12}C_{22} & Y'_{32} &= b_{33}C_{23}\\
Y'_{13} &= b_{11}C_{31} + b_{12}C_{32} & Y'_{33} &= b_{33}C_{33}\\
Y'_{21} &= b_{12}C_{11} + b_{22}C_{12} & &\\
Y'_{22} &= b_{12}C_{21} + b_{22}C_{22} & &\\
Y'_{23} &= b_{12}C_{31} + b_{22}C_{32} & &
\end{aligned}$$

The nine Y'_{ik} values are substituted into (36) to yield explicit values of the six coefficients of f.

$$\begin{aligned}
a_{11} &= b_{11}C_{11}^2 + 2b_{12}C_{11}C_{12} + b_{22}C_{12}^2 + b_{33}C_{13}^2\\
&= f'(C_{11}, C_{12}, C_{13})\\
a_{22} &= b_{11}C_{21}^2 + 2b_{12}C_{21}C_{22} + b_{22}C_{22}^2 + b_{33}C_{23}^2\\
&= f'(C_{21}, C_{22}, C_{23})\\
a_{33} &= b_{11}C_{31}^2 + 2b_{12}C_{31}C_{32} + b_{22}C_{32}^2 + b_{33}C_{33}^2\\
&= f'(C_{31}, C_{32}, C_{33})
\end{aligned}$$

$$a_{12} = b_{11}C_{11}C_{21} + b_{12}C_{11}C_{22} + b_{12}C_{12}C_{21} + b_{22}C_{12}C_{22} + b_{33}C_{13}C_{23}$$

$$a_{13} = b_{11}C_{11}C_{31} + b_{12}C_{11}C_{32} + b_{12}C_{12}C_{31} + b_{22}C_{12}C_{32} + b_{33}C_{13}C_{33}$$

$$a_{23} = b_{11}C_{21}C_{31} + b_{12}C_{21}C_{32} + b_{12}C_{22}C_{31} + b_{22}C_{22}C_{32} + b_{33}C_{23}C_{33}$$

This completes the proof of Theorem 4.

THEOREM 4. <u>Given any integer</u> $d \neq 0$, <u>there exists a form</u>

$$f' = b_{11}y_1^2 + b_{22}y_2^2 + b_{33}y_3^2 + 2b_{12}y_1y_2$$

<u>of determinant</u> $d = b_{33}B_{33}$ <u>and with</u> $(b_{11}, b_{12}) = 1$. <u>The coefficients</u> a_{ij} <u>of a form</u> f <u>equivalent to</u> f' <u>are given by</u>

$$a_{ij} = b_{11}C_{i1}C_{j1} + b_{12}C_{i1}C_{j2} + b_{12}C_{i2}C_{j1} + b_{22}C_{i2}C_{j2} + b_{33}C_{i3}C_{j3} . \tag{37}$$

<u>In particular,</u>

$$a_{ii} = b_{11}C_{i1}^2 + 2b_{12}C_{i1}C_{i2} + b_{22}C_{i2}^2 + b_{33}C_{i3}^2 = f'(C_{i1}, C_{i2}, C_{i3}),$$

<u>where the</u> C_{jk} <u>are the cofactors of the elements</u> c_{jk} <u>of any matrix</u> (c_{jk}) <u>of determinant one</u>.

A numerical example of the application of this theorem is given at the end of this chapter.

Type C: $b_{11} \neq b_{12}$, $(b_{11}, b_{12}) = b > 1$

The construction of a form of type C is accomplished similarly to that of the form of type B.

Let b_{11} and b_{12} be any two distinct integers such that $(b_{11}, b_{12}) = b > 1$. Define b'_{11} and b'_{12} by

(38) $\quad b_{11} = b'_{11}b$, $\quad b_{12} = b'_{12}b$.

Then $(b'_{11}, b'_{12}) = 1$. From the expression for the determinant d of the proposed form

$$f' = b_{11}y_1^2 + b_{22}y_2^2 + b_{33}y_3^2 + 2b_{12}y_1y_2 ,$$

(39) $\quad d = b_{33}B_{33}$, where $B_{33} = b_{11}b_{22} - b_{12}^2$;

hence by (38) and (39), b divides B_{33}. Thus define B'_{33} by $B_{33} = B'_{33}b$. Hence from (38) and (39),

(39') $\quad B'_{33} = b'_{11}b_{22} - b\, b'^2_{12}$.

A necessary and sufficient condition that (39') have integral solutions in b'_{12} and b_{22} for assigned values of B'_{33}, b'_{11}, and b is

(40) $\quad b\, b'^2_{12} \equiv -B'_{33} \pmod{b'_{11}}$.

Define N by

$$b\, N \equiv 1 \pmod{b'_{11}} .$$

Then (40) becomes

$$b_{12}'^{\,2} \equiv -B_{33}' N \qquad (\text{mod } b_{11}')$$

Hence for (40) to have a solution it is necessary that

$$\left(\frac{-B_{33}'N}{b_{11}'}\right) = \left(\frac{-B_{33}'Nb^2}{b_{11}'}\right) = \left(\frac{-B_{33}'b}{b_{11}'}\right) = 1 ,$$

or

(41) $$\left(\frac{b_{11}'}{B_{33}'b}\right) = (-1)^{\frac{B_{33}'b+1}{2}\,\frac{b_{11}'-1}{2}}$$

Take $B_{33}' = 1$. Then given any integer $d \neq 0$, let $B_{33} = b$ be any odd prime factor of d. Since $B_{33}' = 1$, then (41) and Dirichlet's Theorem guarantee the existence of an odd prime $b_{11}' \neq b$. By (38), b_{11} is now fixed in value. Since $B_{33}' = 1$ and (41) is satisfied, then by (40) there must exist an integer b_{12}' satisfying

$$b\, b_{12}' \equiv -1 \qquad (\text{mod } b_{11}')$$

and hence $(b_{11}', b_{12}') = 1$. Relation (38) fixes b_{12} in value, and (39) gives b_{22}. Finally, b_{33} is given by (39). Hence all of the coefficients b_{11}, b_{12}, b_{22}, and b_{33} of f' have been determined. Let C_{jk} be the cofactor of c_{jk} in a unimodular transformation (c_{jk}). Then the coefficients of a form f equivalent to f' of determinant $d \neq 0$ are given by (37).

THEOREM 5. Given any integer $d \neq 0$ which contains as a factor an odd prime, there exists a form

$$f' = b_{11}y_1^2 + b_{22}y_2^2 + b_{33}y_3^2 + 2b_{12}y_1y_2$$

of determinant $d = b_{33}B_{33}$ and with $(b_{11}, b_{12}) = b > 1$. The coefficients of a form f equivalent to f' are given by (37), where the C_{jk} are the cofactors of the elements c_{jk} of any transformation (c_{jk}) of determinant one.

Examples

Let the given determinant be $d = -20$. Forms f equivalent to forms f' of each of types A, B, and C will be constructed. For all of this work the transformation (c_{jk}) will be taken as

$$(c_{jk}) = \begin{pmatrix} -1 & 0 & -1 \\ 7 & 1 & 7 \\ -14 & -2 & -15 \end{pmatrix}$$

Then the matrix of cofactors C_{jk} of the elements c_{jk} is

$$(C_{jk}) = \begin{pmatrix} -1 & 7 & 0 \\ 2 & 1 & -2 \\ 1 & 0 & -1 \end{pmatrix}.$$

The method preceding Theorem 3 is employed for the first construction. Then

$$-20 = b_{11}b_{33} \circ$$

Since b_{11} is any divisor of -20 (there are twelve choices), one might take $b_{11} = 5$. Then $b_{12} = b_{11} = 5$, $b_{22} = 5 + 1 = 6$, and $b_{33} = -4$. By (29), $a_{12} = 97$, $a_{13} = 30$, and $a_{23} = 7$, and by (30), $a_{11} = 229$, $a_{22} = 30$, and $a_{33} = 1$. Hence

$$f = 229x_1^2 + 30x_2^2 + x_3^2 + 194x_1x_2 + 60x_1x_3 + 14x_2x_3.$$

The above form f is the constructed form which is equivalent to a form

$$f' = 5y_1^2 + 6y_2^2 - 4y_3^2 + 10y_1y_2$$

of type A.

For the construction of a form of type B of the same determinant $d = -20$, B_{33} is taken as the odd prime factor $B_{33} = 5$ of d. Then (34) is

$$\left(\frac{b_{11}}{5}\right) = (-1)^{3\left(\frac{b_{11}-1}{2}\right)}$$

which is, when b_{11} is taken as $b_{11} = 3$,

$$\left(\frac{3}{5}\right) = (-1)^3 = -1.$$

Then (32) gives

$$b_{12}^2 \equiv -5 \pmod 3,$$

which is satisfied by $b_{12} = 1$. By (31), $b_{22} = 2$. Finally $b_{33} = d/B_{33} = -20/5 = -4$. Then the coefficients of f' have all been determined. Using the same transformation as in the construction of the form of type A, (37) gives the coefficients of the form f equivalent to f'. The result of this computation

is the form

$$f = 87x_1^2 + 2x_2^2 + 7x_3^2 + 42x_1x_2 + 8x_1x_3 - x_2x_3$$

which is equivalent to the form

$$f' = 3y_1^2 + 2y_2^2 - 4y_3^2 + 2y_1y_2$$

both of which are of determinant $d = -20$.

For the construction of a form of type C, $B_{33} = b = 5$, an odd prime factor of $d = -20$. Relation (41) is now

$$\left(\frac{b'_{11}}{5}\right) = (-1)^{3\left(\frac{b'_{11}-1}{2}\right)} .$$

Take $b'_{11} = 7$, and then by (38), $b_{11} = (7)(5) = 35$. There must exist an integer b'_{12} satisfying

$$5\, b'^{\,2}_{12} \equiv -1 \pmod{7}.$$

Take $b'_{12} = 2$. Then $b_{12} = 10$, by (38). By (39), $b_{22} = 3$. Finally $b_{33} = -4$. Thus the form

$$f' = 35y_1^2 + 3y_2^2 - 4y_3^2 + 20y_1y_2$$

is an example of the form of type C, with $(b_{11}, b_{12}) = (35, 10) = 5 = b > 1$. The desired form f equivalent to f' can be found by (37) in exactly the same manner as the two previous types.

CHAPTER IV

CONDITIONS FOR EQUIVALENCE TO THE FORM f' WITH $b_{23} = 0$, $b_{13} = N$, AND RELATED FORMS

Before conditions for equivalence can be obtained, a preliminary lemma concerning a Diophantine equation must be proved.

LEMMA 4. *All solutions in integers of the non-homogeneous linear Diophantine equation*

$$(42) \qquad a\,x + b\,y + c\,z = d, \quad \textit{where } (a,b,c) \mid d,$$

are given by

$$(43) \qquad \begin{aligned} x &= x_0 + bk - cn \\ y &= y_0 + cs - ak \\ z &= z_0 + an - bs, \end{aligned}$$

where x_0, y_0, z_0 *is any particular solution of (42) and where* s, n, *and* k *are arbitrary integers*.

PROOF. Since x_0, y_0, z_0 is any particular solution of (42), then every solution x, y, z of (42) must satisfy

$$(44) \qquad a(x - x_0) + b(y - y_0) + c(z - z_0) = 0.$$

But by Dickson's <u>Studies in the Theory of Numbers</u>[1] all of the solutions of (44) are given by the second order determinants of the matrix

(45)
$$\begin{pmatrix} a & b & c \\ s & n & k \end{pmatrix},$$

namely

(46)
$$\begin{aligned} x - x_0 &= bk - cn \\ y - y_0 &= cs - ak \\ z - z_0 &= an - bs \quad , \end{aligned}$$

and hence by (43). Moreover, (43) satisfies (42), since

$$a(x_0 + bk - cn) + b(y_0 + cs - ak) + c(z_0 + an - bs) =$$
$$(ax_0 + by_0 + cz_0) + a(bk-cn) + b(cs-ak) + c(an-bs) = d.$$

Since this argument follows for every solution x, y, z of (42), then all solutions of (42) are given by (43).

The information contained in Lemma 4 is to be used in the proof of Lemma 5, which in turn will be employed as a means to the proof of subsequent theorems.

LEMMA 5. <u>A necessary and sufficient condition that the form</u>

$$f = \sum_{i,j=1}^{3} a_{ij}x_i x_j \ , \qquad a_{ji} = a_{ij} \ ,$$

---

[1] <u>Ibid.</u>, p. 24, Theorem 26.

of determinant $d \neq 0$, be equivalent to the form

$$f' = b_{11}y_1^2 + b_{22}y_2^2 + b_{33}y_3^2 + 2b_{12}y_1y_2 + 2Ny_1y_3 ,$$

where N is any preassigned integer, is that the g.c.d. of the values of the three constants

$$(47) \qquad \begin{aligned} &\left\{f_3\left[X'_{33}n - X'_{23}k - c_1\right] + Nc_{13}\right\}, \\ &\left\{f_3\left[X'_{13}k - X'_{33}s - c_2\right] + Nc_{23}\right\}, \\ \text{and } &\left\{f_3\left[X'_{23}s - X'_{13}n - c_3\right] + Nc_{33}\right\} \end{aligned}$$

divide g, where g is defined by (6), s, n, and k are arbitrary, and where $c_{i1} = c_i$, $i = 1,2,3$, is a particular solution of

$$(48) \qquad X'_{13}c_{11} + X'_{23}c_{21} + X'_{33}c_{31} = N .$$

PROOF. Assume that $f \sim f'$. Let c_{13}, c_{23}, c_{33} be the third column of the transformation (c_{jk}) carrying f into f'. Then $(c_{13}, c_{23}, c_{33}) = 1$, for otherwise $c_{jk} \neq 1$, and then $f \not\sim f'$, contrary to hypothesis. By (2), not all of X'_{13}, X'_{23}, and X'_{33} are equal to zero, for then $d = 0$, contrary to hypothesis that $d \neq 0$. Again define X_{13}, X_{23}, and X_{33} as in (6) so that

$$g = (X'_{13}, X'_{23}, X'_{33}).$$

By (1), (48) holds, and therefore $g \mid N$ is a necessary condition that $f \sim f'$. Write

$$(49) \qquad N = gN_1 .$$

If $c_{11} = c_1$, $c_{21} = c_2$, and $c_{31} = c_3$ is a particular solution of (48), then by Lemma 4 all solutions of (48) are given by

$$
\begin{aligned}
c_{11} &= c_1 + X'_{23}k - X'_{33}n \\
c_{21} &= c_2 + X'_{33}s - X'_{13}k \\
c_{31} &= c_3 + X'_{13}n - X'_{23}s \quad ,
\end{aligned}
\tag{50}
$$

where s, n, and k have arbitrary integral values. By (13) and (50), write the values of the cofactors C_{i2} of c_{i2} in (c_{jk}), i= 1,2,3.

$$
\begin{aligned}
C_{12} = {} & c_3c_{23} - c_2c_{33} \\
& -(X'_{23}c_{23} + X'_{33}c_{33})s + (X'_{13}c_{23})n + (X'_{13}c_{33})k \\
C_{22} = {} & c_1c_{33} - c_3c_{13} \\
& +(X'_{23}c_{13})s - (X'_{13}c_{13} + X'_{33}c_{33})n + (X'_{23}c_{33})k \\
C_{32} = {} & c_2c_{13} - c_1c_{23} \\
& +(X'_{33}c_{13})s + (X'_{33}c_{23})n - (X'_{13}c_{13} + X'_{23}c_{23})k
\end{aligned}
\tag{51}
$$

Since

$$
|c_{jk}| = c_{12}C_{12} + c_{22}C_{22} + c_{32}C_{32} = 1,
$$

then

$$
\begin{aligned}
& c_{12}c_3c_{23} - c_{12}c_2c_{33} - (X'_{23}c_{23} + X'_{33}c_{33})c_{12}s \\
& +(X'_{13}c_{23})c_{12}n + (X'_{13}c_{33})c_{12}k + c_{22}c_1c_{33} - c_{22}c_3c_{13} \\
& +(X'_{23}c_{13})c_{22}s - (X'_{13}c_{13} + X'_{33}c_{33})c_{22}n + (X'_{23}c_{33})c_{22}k \\
& + c_{32}c_2c_{13} - c_{32}c_1c_{23} + (X'_{33}c_{13})c_{32}s + (X'_{33}c_{23})c_{32}n \\
& -(X'_{13}c_{13} + X'_{23}c_{23})c_{32}k = 1
\end{aligned}
\tag{52}
$$

or

$$(53)\quad -(X'_{23}c_{23} + X'_{33}c_{33})c_{12}s - (X'_{13}c_{13} + X'_{33}c_{33})c_{22}n$$
$$-(X'_{13}c_{13} + X'_{23}c_{23})c_{32}k + c_{13}s(X'_{23}c_{22} + X'_{33}c_{32})$$
$$+ c_{23}n(X'_{13}c_{12} + X'_{33}c_{32}) + c_{33}k(X'_{13}c_{12} + X'_{23}c_{22}) =$$
$$1 - c_{12}c_3c_{23} + c_{12}c_2c_{33} - c_{22}c_1c_{33} + c_{22}c_3c_{13}$$
$$- c_{32}c_2c_{13} + c_{32}c_1c_{23} \cdot$$

Since $f \sim f'$, then it must be true that

$$(54)\qquad X'_{13}c_{12} + X'_{23}c_{22} + X'_{33}c_{32} = 0 \,.$$

Use (54) to make three substitutions into (53). Then

$$-(X'_{23}c_{23} + X'_{33}c_{33})c_{12}s - (X'_{13}c_{13} + X'_{33}c_{33})c_{22}n$$
$$- (X'_{13}c_{13} + X'_{23}c_{23})c_{32}k - c_{13}s(X'_{13}c_{12}) - c_{23}n(X'_{23}c_{22})$$
$$-c_{33}k(X'_{33}c_{32}) = 1 - c_{12}c_3c_{23} + c_{12}c_2c_{33} - c_{22}c_1c_{33}$$
$$+ c_{22}c_3c_{13} - c_{32}c_2c_{13} + c_{32}c_1c_{23} \cdot$$

The above equation may be multiplied by -1 and factored as

$$c_{12}s(c_{13}X'_{13} + c_{23}X'_{23} + c_{33}X'_{33}) + c_{22}n(c_{13}X'_{13} + c_{23}X'_{23}$$
$$+ c_{33}X'_{33}) + c_{32}k(c_{13}X'_{13} + c_{23}X'_{23} + c_{33}X'_{33}) = c_{12}c_3c_{23}$$
$$- c_{12}c_2c_{33} + c_{22}c_1c_{33} - c_{22}c_3c_{13} + c_{32}c_2c_{13} - c_{32}c_1c_{23} - 1$$

Then relation (3) is employed to obtain

$$(55)\qquad f_3(c_{12}s + c_{22}n + c_{32}k) =$$
$$c_{12}c_3c_{23} - c_{12}c_2c_{33} + c_{22}c_1c_{33}$$
$$- c_{22}c_3c_{13} + c_{32}c_2c_{13} - c_{32}c_1c_{23} - 1.$$

Dividing (54) by g gives

$$X_{13}c_{12} + X_{23}c_{22} + X_{33}c_{32} = 0 ,$$

all solutions of which are given by

$$(56) \qquad \begin{aligned} c_{12} &= X_{23}\gamma - X_{33}\beta \\ c_{22} &= X_{33}\alpha - X_{13}\gamma \\ c_{32} &= X_{13}\beta - X_{23}\alpha , \end{aligned}$$

where α, β, and γ are arbitrary except that their values shall not cause $(c_{12}, c_{22}, c_{32}) > 1$. Substituting (56) into (55), one obtains

$$\begin{aligned} f_3 \Big\{ (X_{23}\gamma - X_{33}\beta)s + (X_{33}\alpha - X_{13}\gamma)n + (X_{13}\beta - X_{23}\alpha)k \Big\} \\ = (X_{23}\gamma - X_{33}\beta)c_3c_{23} - (X_{23}\gamma - X_{33}\beta)c_2c_{33} \\ + (X_{33}\alpha - X_{13}\gamma)c_1c_{33} - (X_{33}\alpha - X_{13}\gamma)c_3c_{13} \\ + (X_{13}\beta - X_{23}\alpha)c_2c_{13} - (X_{13}\beta - X_{23}\alpha)c_1c_{23} - 1. \end{aligned}$$

This last equation may be refactored as

$$\begin{aligned} f_3\Big\{\alpha(X_{33}n - X_{23}k) + \beta(X_{13}k - X_{33}s) + \gamma(X_{23}s - X_{13}n)\Big\} = \\ \alpha\left[c_1(c_{23}X_{23} + c_{33}X_{33}) - c_{13}(c_2X_{23} + c_3X_{33})\right] \\ + \beta\left[c_2(c_{13}X_{13} + c_{33}X_{33}) - c_{23}(c_1X_{13} + c_3X_{33})\right] \\ + \gamma\left[c_3(c_{13}X_{13} + c_{23}X_{23}) - c_{33}(c_1X_{13} + c_2X_{23})\right] - 1 \end{aligned}$$

which, after three substitutions from (48), results in

$$\begin{aligned} f_3\Big\{\alpha(X_{33}n - X_{23}k) + \beta(X_{13}k - X_{33}s) + \gamma(X_{23}s - X_{13}n)\Big\} \\ = \alpha\left[c_1(c_{23}X_{23} + c_{33}X_{33}) + c_{13}(X_{13}c_1 - N_1)\right] \\ + \beta\left[c_2(c_{13}X_{13} + c_{33}X_{33}) + c_{23}(X_{23}c_2 - N_1)\right] \\ + \gamma\left[c_3(c_{13}X_{13} + c_{23}X_{23}) + c_{33}(X_{33}c_3 - N_1)\right] - 1 . \end{aligned}$$

Multiply the above equation by g to obtain

$$f_3\left\{\alpha(X'_{33}n - X'_{23}k) + \beta(X'_{13}k - X'_{33}s) + \gamma(X'_{23}s - X'_{13}n)\right\} =$$
$$\alpha\left[c_1(c_{13}X'_{13} + c_{23}X'_{23} + c_{33}X'_{33}) - c_{13}N\right]$$
$$+ \beta\left[c_2(c_{13}X'_{13} + c_{23}X'_{23} + c_{33}X'_{33}) - c_{23}N\right]$$
$$+ \gamma\left[c_3(c_{13}X'_{13} + c_{23}X'_{23} + c_{33}X'_{33}) - c_{33}N\right] - g ,$$

which, by (3), is

$$f_3\left\{\alpha(X'_{33}n - X'_{23}k) + \beta(X'_{13}k - X'_{33}s) + \gamma(X'_{23}s - X'_{13}n)\right\}$$
$$= \alpha\left[c_1f_3 - c_{13}N\right] + \beta\left[c_2f_3 - c_{23}N\right]$$
$$+ \gamma\left[c_3f_3 - c_{33}N\right] - g$$

or

$$(57)\quad \left\{f_3\left[X'_{33}n - X'_{23}k - c_1\right] + c_{13}N\right\}\alpha$$
$$+\left\{f_3\left[X'_{13}k - X'_{33}s - c_2\right] + c_{23}N\right\}\beta$$
$$+\left\{f_3\left[X'_{23}s - X'_{13}n - c_3\right] + c_{33}N\right\}\gamma = -g$$

Now (57) is a non-homogeneous, linear Diophantine equation in α, β , and γ. A necessary and sufficient condition that integers α, β, and γ exist satisfying (57) is that the g.c.d. of their coefficients divides g. Thus the condition stated in the Lemma is necessary. Moreover, the condition is sufficient, for the steps (48) through (57) may be readily retraced.

COROLLARY 5. A sufficient condition that the form f be equivalent to the form

$$f' = b_{11}y_1^2 + b_{22}y_2^2 + b_{33}y_3^2 + 2b_{12}y_1y_2 + 2Ny_1y_3,$$

where N is any preassigned integer, is that the g.c.d. of the three constants, $Nc_{13} - f_3c_{11}$, $Nc_{23} - f_3c_{21}$, and $Nc_{33} - f_3c_{31}$, divide g, the g.c.d. of the values of the three linear functions X_{i3} defined by (2).

PROOF. Since s, n, and k are arbitrary, take $s = n = k = 0$. Then by (50), $c_{i1} = c_i$, $i = 1,2,3$.

It is of interest to compare the results of Corollary 5 and Lemma 3. For by interchanging the variables y_1 and y_2 of f' and the columns c_{i1} and c_{i2} of (c_{jk}), Corollary 5 states that a sufficient condition that f be equivalent to

$$f' = b_{11}y_1^2 + b_{22}y_2^2 + b_{33}y_3^2 + 2b_{12}y_1y_2 + 2Ny_2y_3$$

is that the g.c.d. of the constants, $Nc_{13} - f_3c_{12}$, $Nc_{23} - f_3c_{22}$, and $Nc_{33} - f_3c_{32}$, divide g. If this be taken as hypothesis, then there exist integers α, β, and γ satisfying

$$(Nc_{13} - f_3c_{12})\alpha + (Nc_{23} - f_3c_{22})\beta + (Nc_{33} - f_3c_{32})\gamma = -g.$$

In the special case of $N = Kb_{33}$, the above becomes

$$(Kb_{33}c_{13} - f_3c_{12})\alpha + (Kb_{33}c_{23} - f_3c_{22})\beta + (Kb_{33}c_{33} - f_3c_{32})\gamma = -g,$$

and since by Lemma 1, $f_3 = b_{33}$, the latter is rewritten as

$$f_3\left\{(Kc_{13} - c_{12})\alpha + (Kc_{23} - c_{22})\beta + (Kc_{33} - c_{32})\gamma\right\} = -g.$$

Hence f_3 divides g. But g divides each term of $f_3 = b_{33}$, by (2) and (6), and hence divides f_3. Thus f_3 equals g or -g, exactly the condition of Lemma 3. Thus in the special case of $N = Kb_{33}$ the results of the two separate statements are seen to agree. Therefore Lemma 3 may in a sense be considered as a special case of Corollary 5.

Throughout this study the three linear functions (4), namely,

$$X_s' = X_s'(x_1, x_2, x_3) = a_{s1}x_1 + a_{s2}x_2 + a_{s3}x_3, \quad s = 1,2,3,$$

have been of great value in obtaining conditions for the equivalence of two forms. The functions X_s' are said to be <u>associated with the form</u>

$$f = \sum_{i,j=1}^{3} a_{ij}x_i x_j, \qquad a_{ji} = a_{ij} ,$$

<u>i.e.</u>, given any form f, the functions X_s' are defined by (4). A complete change of viewpoint yields the following statement: given any three linear functions X_s' , as defined by (4), there is associated a form

$$f = \sum_{i,j=1}^{3} a_{ij}x_i x_j ,$$

or, in other words, the form is said to be <u>associated with the functions</u>. This novel viewpoint is of some interest and is found to be helpful in the proof of further theorems later in this chapter, notably Theorem 6. The idea of associating a form with a set of three given functions X_s' raises one diffi-

culty, however, namely, that a form f so associated with the functions X_s' may not be a classic form, i.e., it may not be true that $a_{ji} = a_{ij}$, $i \neq j$, $i,j = 1,2,3$. Up to the present point in this dissertation only classic forms have been studied. Hence a few definitions and minor lemmas concerning non-classic forms are required and are now presented.

In Chapter I the divisors τ and σ of the classic form

$$f = \sum_{i,j=1}^{3} a_{ij}x_i x_j, \qquad a_{ji} = a_{ij} ,$$

were defined by

$$\tau = (a_{11}, a_{12}, a_{13}, a_{22}, a_{23}, a_{33})$$

and $$\sigma = (a_{11}, a_{22}, a_{33}, 2a_{12}, 2a_{13}, 2a_{23}).$$

If $\tau = 1$, then f is a primitive form, and then $\sigma = 1$ or 2. When $\sigma = 1$, f is properly primitive, and when $\sigma = 2$, f is improperly primitive.

Analogous definitions for the non-classic form are

$$\tau = (a_{11}, a_{12}, a_{13}, a_{21}, a_{22}, a_{23}, a_{31}, a_{32}, a_{33})$$

and $$\sigma = (a_{11}, a_{22}, a_{33}, a_{12}+a_{21}, a_{13}+a_{31}, a_{23}+a_{32}).$$

It is seen that the second set of definitions includes the first set as a special case. If $\tau = 1$, f is primitive; then the value of σ is not restricted to 1 or 2, as in the classic case. If $\tau = 1$ and $\sigma > 1$, then f is improperly primitive. If $\sigma = 1$, then $\tau = 1$, and f is said to be properly

primitive.

In Dickson's Studies in the Theory of Numbers Theorem 6 states that any properly primitive (classic, n-ary quadratic) form represents primitively some integer prime to any assigned integer m.[2] A similar statement holds for ternary non-classic forms.

LEMMA 6. Any properly primitive classic or non-classic form q represents primitively an integer prime to any assigned integer m.

PROOF. The statement for the classic case is proved by Dickson.[3] The proof given by him suffices with slight modifications for the non-classic case. A shorter proof will be presented, however. Since q is a non-classic properly primitive form, then $f = 2q$ is a classic improperly primitive form. By Theorem 7, Dickson's Studies in the Theory of Numbers, f represents primitively the double of an odd integer prime to any assigned integer m.[4] Let 2N be the integer so represented by f and such that $(m, N) = 1$. Since $2q = f$ represents 2N primitively, then q represents N primitively.

LEMMA 7. If a classic or non-classic form f represents A primitively, then f is equivalent to a form having A as the coefficient of y_1^2.

---

[2] Ibid., p. 8. [3] Ibid. [4] Ibid.

PROOF. The classic case is given by Dickson,[5] and the non-classic case is mentioned by Sagen.[6] Both cases are proved here. Since f represents A primitively, there exists a primitive set such that $f(c_{11}, c_{21}, c_{31}) = A$ with $(c_{11}, c_{21}, c_{31}) = 1$. By Theorem 123, Modern Elementary Theory of Numbers, there exists a determinant with integral elements having the value one and having c_{11}, c_{21}, c_{31} as the elements in the first column.[7] Denote the matrix of this determinant by (c_{jk}), $j,k = 1,2,3$. Apply to the form f the unimodular transformation associated with the matrix (c_{jk}). The resulting equivalent form f' has coefficients b_{sk}, where, by (3), which holds for classic and non-classic forms, the value of b_{11} is $b_{11} = f(c_{11}, c_{21}, c_{31}) = A$.

The forthcoming Theorem 6 has been proved, with slightly different hypothesis, for n linear functions in n + m indeterminates by H. J. S. Smith.[8] It is stated in this study for the sake of clarity and for its application to the theory of forms. Smith's method of proof is used in part of Lemma 8 below.

---

[5] Ibid., p. 12.

[6] O. K. Sagen, The Integers Represented by Sets of Positive Ternary Quadratic Non-classic Forms, (Chicago,) 1936, p.2.

[7] L. E. Dickson, Modern Elementary Theory of Numbers, (Chicago,) 1939, p. 172.

[8] J. W. L. Glaisher (ed.), The Collected Mathematical Papers of Henry John Stephen Smith, (Oxford,) 1894, I, 392-393.

LEMMA 8. Let Ω denote the g.c.d. of the literal coefficients A_{ij} of the adjoint ϕ of the properly primitive classic or non-classic form f of non-zero determinant d. If the leading coefficient a_{11} of f is relatively prime to the integer d/Ω, then there exists a primitive set x_1', x_2', x_3' of values of the indeterminates x_1, x_2, x_3 for which the g.c.d. of the three linear functions

$$
\begin{aligned}
X_1' &= a_{11}x_1 + a_{12}x_2 + a_{13}x_3 \\
X_2' &= a_{21}x_1 + a_{22}x_2 + a_{23}x_3 \\
X_3' &= a_{31}x_1 + a_{32}x_2 + a_{33}x_3 ,
\end{aligned} \tag{58}
$$

associated with the form f, is one.

PROOF. First it will be shown that the values of x_1, x_2, and x_3 can be so chosen that the g.c.d. of the three X_i', $i = 1,2,3$, is prime to some given integer M, provided only that M is prime to a_{11}. For assign to x_1, x_2, x_3 the values $x_1 = 1$, $x_2 = M$, $x_3 = M$. When these values are placed in (58), the value of X_1' is prime to M, for the first term of X_1' is prime to M, and the second two terms are multiples of M. Since $(X_1', M) = 1$, then the g.c.d. of the values of the three X_i' is prime to M, for, otherwise, a divisor of X_1' is not prime to M, a contradiction.

A method has been outlined to obtain a set of values C_1, C_2, C_3 of X_1', X_2', X_3' respectively, satisfying

$$(59) \qquad \begin{aligned} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 &= C_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 &= C_2 \\ a_{31}x_1 + a_{32}x_2 + a_{33}x_3 &= C_3 \end{aligned}$$

and such that $(C_1, C_2, C_3) = C$ is prime to some assigned integer M, provided only that $(a_{11}, M) = 1$. A similar result follows if the hypothesis is taken that any a_{ij} is prime to M, but this latter result is not required for the purpose of this lemma.

Let A_{ij} be the cofactor of a_{ij} in (a_{ij}). Ω has been defined as

$$\Omega = (A_{11}, A_{12}, A_{13}, A_{21}, A_{22}, A_{23}, A_{31}, A_{32}, A_{33}).$$

It is well known that

$$d = \Omega^2 \Delta,$$

where Ω and Δ are invariants of the form f. Hence $\Omega \mid d$. Write

$$M = d/\Omega .$$

Then there exist integers x_1, x_2, x_3 satisfying (59) and for which the g.c.d. C of C_1, C_2, C_3 is prime to d/Ω.

Define d_1, d_2, and d_3 by

$$d_1 = \begin{vmatrix} C_1 & a_{12} & a_{13} \\ C_2 & a_{22} & a_{23} \\ C_3 & a_{32} & a_{33} \end{vmatrix},$$

$$d_2 = \begin{vmatrix} a_{11} & C_1 & a_{13} \\ a_{21} & C_2 & a_{23} \\ a_{31} & C_3 & a_{33} \end{vmatrix},$$

$$d_3 = \begin{vmatrix} a_{11} & a_{12} & C_1 \\ a_{21} & a_{22} & C_2 \\ a_{31} & a_{32} & C_3 \end{vmatrix}.$$

It has been shown explicitly that the system (59) is satisfied in integers. But by the Theorem of Heger, a necessary and sufficient condition that (59) has integral solutions is that d divides each of d_1, d_2, and d_3; i.e., the value of the determinant d must divide each of the three "augmented" determinants.[9] Write

$$\begin{aligned} d_1 &= A_{11}C_1 + A_{21}C_2 + A_{31}C_3 \\ d_2 &= A_{12}C_1 + A_{22}C_2 + A_{32}C_3 \\ d_3 &= A_{13}C_1 + A_{23}C_2 + A_{33}C_3 . \end{aligned}$$

The g.c.d. of the nine A_{ij} is Ω, and the g.c.d. of the three C_i is C, so that ΩC must divide each term of d_1, d_2, and d_3, and hence ΩC divides each of the d_i, $i = 1,2,3$. Therefore there exist integers θ_1, θ_2, and θ_3 such that

$$\begin{aligned} d_1 &= \theta_1 C \Omega \\ d_2 &= \theta_2 C \Omega \\ d_3 &= \theta_3 C \Omega . \end{aligned}$$

---

[9] Ibid., p. 387.

The necessary and sufficient condition that (59) has integral solutions, namely, that d divides each of d_1, d_2, and d_3, can now be stated as

$$(60) \qquad d \,\Big|\, \theta_i C \Omega , \qquad i = 1,2,3,$$

and since Ω divides d, then (60) is tantamount to

$$(61) \qquad \frac{d}{\Omega} \,\Big|\, \theta_i C \quad , \qquad i = 1,2,3.$$

It has been shown that (59) has integral solutions and that by the Theorem of Heger a necessary condition that (59) has integral solutions is that (61) holds. Hence (61) is necessary. But $(d/\Omega , C) = 1$, so that

$$(62) \qquad \frac{d}{\Omega} \,\Big|\, \theta_i \quad , \qquad i = 1,2,3,$$

which is

$$(63) \qquad d \,\Big|\, \theta_i \Omega = d_i/C , \quad i = 1,2,3.$$

But this last statement, that d divides each of d_1/C, d_2/C, and d_3/C, is, by the Theorem of Heger, precisely the condition that the system

$$(64) \qquad \begin{aligned} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 &= C_1/C \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 &= C_2/C \\ a_{31}x_1 + a_{32}x_2 + a_{33}x_3 &= C_3/C \end{aligned}$$

be satisfied in integers. Therefore there exist integers $x_1 = x_1'$, $x_2 = x_2'$, $x_3 = x_3'$ which satisfy (64), and thus, since

$(C_1/C,\ C_2/C,\ C_3/C) = 1$, it may now be said that there exist integers $x_i = x_i'$ for which the g.c.d. of the values of the three X_i', defined by (58), is one. Moreover, the set x_1', x_2', x_3' is itself a primitive set, for if $(x_1', x_2', x_3') = h > 1$, then by (58), h divides each of X_i', contrary to the proven fact that $(X_1', X_2', X_3') = 1$.

THEOREM 6. If $(a_{11}, a_{22}, a_{33}, a_{12}+a_{21}, a_{13}+a_{31}, a_{23}+a_{32}) = 1$, then there exists a primitive set $x_1 = x_1'$, $x_2 = x_2'$, $x_3 = x_3'$ for which the g.c.d. of the three linear functions (58)

$$
\begin{aligned}
X_1' &= a_{11}x_1 + a_{12}x_2 + a_{13}x_3 \\
X_2' &= a_{21}x_1 + a_{22}x_2 + a_{23}x_3 \\
X_3' &= a_{31}x_1 + a_{32}x_2 + a_{33}x_3
\end{aligned}
$$

is one.

PROOF. Associated with the set (58) of linear functions is the not necessarily classic form

$$f = \sum_{i,j=1}^{3} a_{ij}x_ix_j$$

Compute d/Ω as defined in Lemma 8. If $(a_{11}, d/\Omega) = 1$, then by Lemma 8 there exist integers for which the g.c.d. of the three $X_i'(x_1', x_2', x_3')$, $i = 1,2,3$, is one. Also by Lemma 8 the x_i' constitute a primitive set. The only other case arises when $(a_{11}, d/\Omega) \neq 1$. By hypothesis, $\sigma = 1$, and hence f is properly primitive. By Lemma 6, f primitively represents an

integer prime to d/Ω. Denote this primitively represented integer prime to d/Ω by N. By Lemma 7, f is equivalent to a form f' whose first coefficient is N. Associated with the form f' is a set of three linear functions defined by

(65)
$$\begin{aligned} Y_1' &= b_{11}y_1 + b_{12}y_2 + b_{13}y_3 \\ Y_2' &= b_{21}y_1 + b_{22}y_2 + b_{23}y_3 \\ Y_3' &= b_{31}y_1 + b_{32}y_2 + b_{33}y_3, \end{aligned}$$

where $b_{11} = N$ is prime to the arithmetic invariant d/Ω. The transformation (c_{jk}) sending f into f' is given by

(66)
$$\begin{aligned} x_1 &= c_{11}y_1 + c_{12}y_2 + c_{13}y_3 \\ x_2 &= c_{21}y_1 + c_{22}y_2 + c_{23}y_3 \\ x_3 &= c_{31}y_1 + c_{32}y_2 + c_{33}y_3, \end{aligned}$$

where $|c_{jk}| = 1$. By Lemma 8, since f' is properly primitive and since $(b_{11}, d/\Omega) = 1$, there exist integers $y_1 = y_1'$, $y_2 = y_2'$, $y_3 = y_3'$ for which the g.c.d. of the values of the three linear functions Y_i', $i = 1,2,3$, is one. A well known relation between the functions X_i' of (58) and Y_i' of (65) is

(67)
$$Y_s' = X_1'c_{1s} + X_2'c_{2s} + X_3'c_{3s}, \qquad s = 1,2,3.$$

By (66), obtain the values x_1', x_2', x_3' corresponding to the y_i' values. Then the three integers x_i' so derived cause the g.c.d. of the values of the three X_i' to be one. For assume that $(X_1', X_2', X_3') = g > 1$ with the values x_i', $i = 1,2,3$. Then

by (67), g divides each corresponding Y_1', Y_2', and Y_3', a contradiction that their g.c.d. is one. Therefore given any set of functions (58) with the restrictions of the hypothesis, then there exists a primitive set x_1', x_2', x_3' for which the g.c.d. of the values of the three linear functions (58) is one.

It is worthy of note that although the entire proof of Theorem 6 is based upon properties of quadratic forms, the statement of the Theorem itself includes no reference to forms. In other words, the concept of quadratic forms has been completely divorced from the three linear functions (58), and Theorem 6 is simply a theorem concerning a system of linear Diophantine equations with certain restrictions on the nine coefficients.

THEOREM 7. Every ternary quadratic form

$$f = \sum_{i,j=1}^{3} a_{ij}x_ix_j , \qquad a_{ji} = a_{ij} ,$$

of determinant $d \neq 0$ is equivalent to some form

$$f' = b_{11}y_1^2 + b_{22}y_2^2 + b_{33}y_3^2 + 2b_{12}y_1y_2 + 2b_{23}y_2y_3 .$$

PROOF. Given any general ternary quadratic form f of nonzero determinant, a method will be given whereby a transformation (c_{jk}) of determinant $|c_{jk}| = 1$ can be obtained which

sends f into a form f' with $b_{13} = 0$. Let c_{13}, c_{23}, c_{33} be particular primitive set $c_{13} = c_{23} = c_{33} = 1$. Then by (2), not all of the three linear functions X'_{i3}, $i = 1,2,3$, are equal to zero, for then $d = 0$, contrary to hypothesis. Use of (6) gives the value of g and the three numerical values X_{i3}, $i = 1,2,3$. If f is to be equivalent to f', then by (7),

$$X_{13}c_{11} + X_{23}c_{21} + X_{33}c_{31} = 0$$

must hold, and all values, not all zero, of c_{11}, c_{21}, c_{31} for which (7) holds are given by (8), namely,

$$\begin{aligned} c_{11} &= X_{23}k - X_{33}n \\ c_{21} &= X_{33}s - X_{13}k \\ c_{31} &= X_{13}n - X_{23}s \quad , \end{aligned}$$

where the s, n, and k are arbitrary. In the proposed transformation (c_{jk}) the cofactors C_{i2} of the elements c_{i2} are given by (13), (14), and, since $c_{13} = c_{23} = c_{33} = 1$, by

$$\begin{aligned} C_{12} &= (X_{13})k - (X_{23} + X_{33})s + (X_{13})n \\ C_{22} &= (X_{23})k + (X_{23})s - (X_{13} + X_{33})n \\ C_{32} &= -(X_{13} + X_{23})k + (X_{33})s + (X_{33})n \ . \end{aligned} \tag{68}$$

Now the three cofactors given by (68) may be considered as three linear functions in k, s, and n, for the X_{i3} are fixed numbers while the k, s, and n are completely arbitrary. By Theorem 6, since $(X_{13}, X_{23}, X_{33}) = 1$, then there exist inte-

gers $k = k'$, $s = s'$, $n = n'$ for which the g.c.d. of the three cofactors C_{12}, C_{22}, and C_{32} is one. Moreover the values k', s', and n' when placed in (8) give a primitive set of values of c_{11}, c_{21}, and c_{31}, for, if not, then by (13) the cofactors C_{12}, C_{22}, and C_{32} are not a primitive set, an obvious contradiction.

The values c_{13}, c_{23}, c_{33} were chosen as 1, 1, 1; the of c_{11}, c_{21}, c_{31} are now fixed by the choice of s, n, k as s', n', k', respectively. It was shown that the cofactors C_{12}, C_{22}, C_{32} given by (68) form a primitive set. Hence there exist integers c_{12}, c_{22}, c_{32} satisfying (5), which is

$$c_{12}C_{12} + c_{22}C_{22} + c_{32}C_{32} = 1.$$

Moreover, c_{12}, c_{22}, c_{32} is a primitive set by (5).

A transformation (c_{jk}) of determinant one has been obtained satisfying (7). Hence if (c_{jk}) be applied to f, then f is sent into a form with $b_{13} = 0$, which is precisely the identifying feature of f'.

Lemma 9 concerns the non-homogeneous linear Diophantine equation of Lemma 4.

LEMMA 9. <u>If</u> $(a,b,c) = 1$, <u>then there exists a primitive solution</u> x', y', z' <u>of the non-homogeneous linear Diophantine equation (42)</u>,

$$a\,x + b\,y + c\,z = d,$$

<u>for any integer</u> $d \neq 0$.

PROOF. When $d = 1$, the statement is trivially true. Hence consider $d \neq 1$. Since $(a,b,c) = 1$, then there exist solutions of

$$ax + by + cz = 1. \tag{69}$$

Let one such solution of (69) be $x = x_0$, $y = y_0$, $z = z_0$. Since $(a,b,c) \mid d$ for any integer d, there exist solutions of (42). In fact one such (non-primitive) solution of (42) is $x = dx_0$, $y = dy_0$, $z = dz_0$. By Lemma 4, since dx_0, dy_0, dz_0 is a particular solution of (42), then all solutions of (42) are given by

$$\begin{aligned} x &= dx_0 + bk - cn \\ y &= dy_0 + cs - ak \\ z &= dz_0 + an - bs \ , \end{aligned} \tag{70}$$

where s, n, and k are arbitrary. Define U_1, U_2, and U_3 by

$$\begin{aligned} U_1 &= x - dx_0 \\ U_2 &= y - dy_0 \\ U_3 &= z - dz_0 \ . \end{aligned} \tag{71}$$

Then (70), after rearrangement, becomes

$$\begin{aligned} U_1 &= (\ b)k + (\ 0)s + (-c)n \\ U_2 &= (-a)k + (\ c)s + (\ 0)n \\ U_3 &= (\ 0)k + (-b)s + (\ a)n \ . \end{aligned} \tag{72}$$

By Theorem 6, since $(a,b,c) = 1$, there exist integers $s = s'$, $n = n'$, $k = k'$ for which the values of the U_i, $i = 1,2,3$, form a primitive set. Place these integers s', n', and k' into (70). Then by Lemma 4 the resulting values x', y', z' of x, y, and z are solutions of (42). Moreover, x',y',z' is a primitive set, for if $(x',y',z') = h>1$, then by (42), $h \mid d$, and thus by (71) h divides each U_i, a contradiction. Hence there exists a primitive solution x', y', z' of (42).

CONJECTURE: <u>Any properly primitive form</u>

$$f = \sum_{i,j=1}^{3} a_{ij}x_ix_j, \qquad a_{ji} = a_{ij},$$

<u>of determinant</u> $d \neq 0$ <u>is equivalent to some form</u>

$$f' = b_{11}y_1^2 + b_{22}y_2^2 + b_{33}y_3^2 + 2Ny_1y_2 + 2b_{13}y_1y_3 + 2b_{23}y_2y_3,$$

<u>where</u> N <u>is any preassigned integer</u>.

REMARKS. Since f is properly primitive, then the three linear functions

$$\text{(73)} \qquad \begin{aligned} X'_{12} &= a_{11}c_{12} + a_{12}c_{22} + a_{13}c_{32} \\ X'_{22} &= a_{12}c_{12} + a_{22}c_{22} + a_{23}c_{32} \\ X'_{32} &= a_{13}c_{12} + a_{23}c_{22} + a_{33}c_{32} \end{aligned}$$

associated with the form f and defined by (2) possess coefficients which satisfy the hypothesis of Theorem 6, which is to say that $\sigma = 1$. Hence there exist integers $c_{12} = c'_{12}$, $c_{22} =$

c'_{22}, $c_{32} = c'_{32}$ for which the g.c.d. of the values of X'_{12}, X'_{22}, and X'_{32} is one. Also, by Theorem 6, $(c'_{12}, c'_{22}, c'_{32}) = 1$. Consider the equation

$$X'_{12}c_{11} + X'_{22}c_{21} + X'_{32}c_{31} = N. \tag{74}$$

A sufficient condition that (74) have solutions is that $(X'_{12}, X'_{22}, X'_{32}) = 1$. Moreover, by Lemma 9, since $(X'_{12}, X'_{22}, X'_{32}) = 1$, (74) possesses a primitive solution c'_{11}, c'_{21}, c'_{31}. Now if the three cofactors C_{13}, C_{23}, and C_{33} defined by

$$\begin{aligned} C_{13} &= c'_{21}c'_{32} - c'_{31}c'_{22} \\ C_{23} &= c'_{31}c'_{12} - c'_{11}c'_{32} \\ C_{33} &= c'_{11}c'_{22} - c'_{21}c'_{12} \end{aligned} \tag{75}$$

comprise a primitive set, then there exist integers c_{13}, c_{23}, c_{33} such that $|c_{jk}| = 1$. From the infinitude of possible choices for the sets c_{i1} and c_{i2}, $i = 1,2,3$, there seems to be nothing which would preclude obtaining a primitive set of cofactors (75). However, it has not been proved that such a choice is in every case possible. The writer has found no counter-example. The problem of attempting to show that such a choice is always possible (and hence that any properly primitive form f of non-zero determinant is equivalent to some f') is of considerable complexity.

LEMMA 10. <u>The form</u>

$$f = x_1^2 + a_{22}x_2^2 + a_{33}x_3^2 + 2a_{12}x_1x_2 + 2a_{13}x_1x_3 + 2a_{23}x_2x_3$$

<u>of determinant</u> $d \neq 0$ <u>is equivalent to some form</u>

$$f' = b_{11}y_1^2 + b_{22}y_2^2 + y_3^2 + 2b_{12}y_1y_2 + 2Ny_1y_3 ,$$

<u>where</u> N <u>is any preassigned integer</u>.

PROOF. Assign to c_{13}, c_{23}, c_{33} the values $c_{13} = 1$, $c_{23} = 0$, and $c_{33} = 0$. Then by (2), $X'_{13} = 1$, $X'_{23} = a_{12}$, $X'_{33} = a_{13}$, so that by (6), $g = 1$, and $X'_{i3} = X_{i3}$, $i = 1,2,3$. Define by (49), $N_1 = N/g = N$. By (3), $f_3 = f(1, 0, 0) = 1$. Assign to c_{11}, c_{21}, c_{31} the values $c_{11} = N - a_{13}$, $c_{21} = 0$, and $c_{31} = 1$. Then $(c_{11}, c_{21}, c_{31}) = 1$. The cofactors C_{i2} of c_{i2} are

$$\begin{aligned} C_{12} &= 0 \\ C_{22} &= -1 \\ C_{32} &= 0 , \end{aligned} \tag{76}$$

a primitive set. The values of the three expressions, $Nc_{i3} - f_3c_{i1}$, $i = 1,2,3$, of Corollary 5 are

$$\begin{aligned} Nc_{13} - f_3c_{11} &= N(1) - 1(N - a_{13}) = a_{13} \\ Nc_{23} - f_3c_{21} &= N(0) - 1(0) \quad\quad\;\; = 0 \\ Nc_{33} - f_3c_{31} &= N(0) - 1(1) \quad\quad\;\; = -1 , \end{aligned} \tag{77}$$

and since their g.c.d. is one and hence divides g, then, by Corollary 5, f is equivalent to a form having $b_{23} = 0$ and $b_{13} = N$. By (3), $b_{33} = f_3 = 1$. Hence $f \sim f'$. Lemma 10 is now

proved. However it may be desired to have at hand an explicit transformation carrying f into f' for purposes of later reference. Thus by (57) and (77),

$$(a_{13})\alpha + (0)\beta + (-1)\gamma = -1, \tag{78}$$

and a suitable set of values satisfying (78) is

$$\alpha = 0, \quad \beta = 0, \quad \gamma = 1. \tag{79}$$

By (79) and (56), $c_{12} = a_{12}$, $c_{22} = -1$, and $c_{32} = 0$. Thus a transformation sending f into f' is given by

$$(c_{jk}) = \begin{pmatrix} N-a_{13} & a_{12} & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}. \tag{80}$$

That transformation (80) is of determinant one is evident. Moreover, by computation, (48) and (54) hold.

THEOREM 8. Any properly primitive form f of determinant $d \neq 0$ which primitively represents one is equivalent to

$$f' = b_{11}y_1^2 + b_{22}y_2^2 + y_3^2 + 2b_{12}y_1y_2 + 2Ny_1y_3,$$

where N is any preassigned integer.

PROOF. By Lemma 7, f is equivalent to a form

$$f^* = x_1^2 + a_{22}x_2^2 + a_{33}x_3^2 + 2a_{12}x_1x_2 + 2a_{13}x_1x_3 + 2a_{23}x_2x_3 .$$

By Lemma 10, $f^{\#} \sim f'$. Therefore, $f \sim f'$.

COROLLARY 6. <u>Any properly primitive form</u> f <u>of determinant</u> $d \neq 0$ <u>which primitively represents one is equivalent to the form</u>

$$f'' = b_{11}y_1^2 + b_{22}y_2^2 + y_3^2 + 2b_{12}y_1y_2 + 2y_1y_3 .$$

PROOF. By Theorem 8, $f \sim f'$ with N any preassigned integer. Let N equal one.

Examples

The form of the title of this chapter, *i.e.*, the form f' with $b_{13} = N$, $b_{23} = 0$, possesses rather complex conditions that a general form f be equivalent to f'. These conditions as given in Lemma 5 are quite explicit but nevertheless cumbersome. However, if the relations (47) through (57) be considered as a set of working equations whereby given any form f, a form f' equivalent to f can be obtained, if such a form f' exists, then Lemma 5 is quite useful. Consider the reduced, positive form

$$f = 2x_1^2 + 3x_2^2 + 5x_3^2 + 2x_1x_2 + 2x_1x_3 + 2x_2x_3$$

of determinant $d = 22$. If there should exist a form f' with $b_{13} = N$, $b_{23} = 0$, which is equivalent to f, where N is arbitrary, then such a form f' can be obtained by Lemma 5. Let $N = 17$. By (2),

$$X'_{13} = 2c_{13} + c_{23} + c_{33}$$

$$X'_{23} = c_{13} + 3c_{23} + c_{33}$$
$$X'_{33} = c_{13} + c_{23} + 5c_{33} ,$$

and by Theorem 6 there exist values of c_{13}, c_{23}, c_{33} such that $g = 1$. Such a set of values is $c_{13} = 5$, $c_{23} = 4$, and $c_{33} = 3$. Then by (2) and (6), $X'_{13} = 17$, $X'_{23} = 20$, $X'_{33} = 24$, $g = 1$, $X_{13} = 17$, $X_{23} = 20$, and $X_{33} = 24$. By (49), $N_1 = 17$. Relation (48) now becomes

$$17c_{11} + 20c_{21} + 24c_{31} = 17,$$

one solution of which is $c_1 = 1$, $c_2 = 0$, $c_3 = 0$. The values of the three constants (47) are

$$237\ (24n - 20k - 1) + 85$$
$$237\ (17k - 24s) + 68$$
$$237\ (20s - 17n) + 51 ,$$

and, taking $s = n = k = 0$, the expressions (47) have respective values -152, 68, and 51, whose g.c.d. is one. By (57),

$$-152\alpha + 68\beta + 51\gamma = -1 ,$$

one of whose solutions is $\alpha = -1$, $\beta = 0$, and $\gamma = -3$. By (56), $c_{12} = -60$, $c_{22} = 27$, and $c_{32} = 20$. Hence the transformation

$$(c_{jk}) = \begin{pmatrix} 1 & -60 & 5 \\ 0 & 27 & 4 \\ 0 & 20 & 3 \end{pmatrix}$$

of determinant one sends f into the desired form f'. By matrix computation,

$$(f') = \begin{pmatrix} 1 & 0 & 0 \\ -60 & 27 & 20 \\ 5 & 4 & 3 \end{pmatrix} \begin{pmatrix} 0 & 1 & 1 \\ 1 & 3 & 1 \\ 1 & 1 & 5 \end{pmatrix} \begin{pmatrix} 1 & -60 & 5 \\ 0 & 27 & 4 \\ 0 & 20 & 3 \end{pmatrix} =$$

$$\begin{pmatrix} 2 & 1 & 1 \\ -73 & 41 & 67 \\ 17 & 20 & 24 \end{pmatrix} \begin{pmatrix} 1 & -60 & 5 \\ 0 & 27 & 4 \\ 0 & 20 & 3 \end{pmatrix} = \begin{pmatrix} 2 & -73 & 17 \\ -73 & 6827 & 0 \\ 17 & 0 & 237 \end{pmatrix},$$

so that the desired form f' is

$$f' = 2y_1^2 + 6827y_2^2 + 237y_3^2 - 146y_1y_2 + 34y_1y_3 .$$

No examples are given here of Theorem 7 since its application is similar to that of Lemma 5, which was just illustrated.

Lemma 10 has an interesting application. For given any form f of the type described in the statement of the Lemma, not only does there exist a form f' equivalent to f and with $b_{33} = 1$, $b_{13} = N$, $b_{23} = 0$, but one can find the form f' immediately by applying to f the transformation (80). Take as the form f

$$f = x_1^2 + 3x_2^2 + 5x_3^2 + 6x_1x_2 + 2x_1x_3 + 10x_2x_3 ,$$

and let N = 11. Then by (80),

$$(c_{jk}) = \begin{pmatrix} 10 & 3 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Application of (c_{jk}) to f gives the form

$$f' = 125y_1^2 - 6y_2^2 + y_3^2 - 4y_1y_2 + 22y_1y_3$$

of the desired type.

CHAPTER V

CONDITIONS FOR EQUIVALENCE TO THE FORM f' WITH $b_{13} = 0$, $b_{23} = M$, AND RELATED FORMS

If one is given a form f and the problem to determine whether f is equivalent to

$$f' = b_{11}y_1^2 + b_{22}y_2^2 + b_{33}y_3^2 + 2b_{12}y_1y_2 + 2My_2y_3 ,$$

one should first determine whether M is a multiple of b_{33}. If $M = Kb_{33}$, then conditions for equivalence of f and f' may be found in Lemma 3. If M is not a multiple of b_{33}, then apply to f' the transformation

$$(81) \qquad \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

to obtain the equivalent form

$$f'' = b_{22}z_1^2 + b_{11}z_2^2 + b_{33}z_3^2 + 2b_{12}z_1z_2 - 2Mz_1z_3 ,$$

which, after suitable changes of notation, is treated in Lemma 5 and Corollary 5. In both of these separate cases, i.e., Lemmas 3 and 5, necessary and sufficient conditions for equivalence of f and f' are given. Throughout this dissertation various necessary conditions and sufficient conditions for equivalence are given separately.

Given a form f as above, the problem of determining whether f is equivalent to some form f' is far from a routine matter. In the summary of this study a reference table will be furnished whereby the student may locate applicable tests for equivalence more readily. If no theorem, lemma, or corollary of this dissertation seems to apply to the problem at hand, suitable interchanges of variables, as accomplished by (81), may yield results.

Two rather obvious but sometimes overlooked suggestions are made: (1) if testing whether f and f' are equivalent seems hopeless, interchange f with f', i.e., attempt to determine conditions that f' be equivalent to f rather than that f be equivalent to f'; (2) if the problem is still unresolved, then compute the adjoints ϕ and ϕ' of f and f' respectively, for $f \sim f'$ if and only if $\phi \sim \phi'$.

CHAPTER VI

CONDITIONS FOR EQUIVALENCE TO THE FORM f' WITH $b_{12} = b_{13} = b_{23} = 0$

Professor E. H. Hadlock will present to the American Mathematical Society the following theorem, which is stated here because of its usefulness in the further development of the theory of equivalence.

THEOREM. <u>A necessary condition that there will exist a linear transformation</u> (c_{jk}) <u>with</u> $|c_{jk}| = 1$, $j,k = 1,2,3$, <u>which will take the form</u>

$$f = \sum_{i,j=1}^{3} a_{ij} x_i x_j , \qquad a_{ji} = a_{ij} ,$$

<u>into the equivalent form</u>

$$f' = b_{11} y_1^2 + b_{22} y_2^2 + b_{33} y_3^2$$

<u>is that</u> f <u>represents primitively a divisor</u> f_3 <u>of</u> d, <u>where</u> $|f_3|$ <u>equals</u> $g = (X'_{13}, X'_{23}, X'_{33})$, <u>and where</u>

$$X'_{13} = a_{11} c_{13} + a_{12} c_{23} + a_{13} c_{33} , \quad i = 1,2,3.$$

<u>A necessary and sufficient condition for the equivalence of</u> f <u>and</u> f' <u>is that there exist integral values of</u> α_1,

α_2, α_3 for which $|U|$, as defined by

$$\text{(i)} \qquad U = U(\alpha_1, \alpha_2, \alpha_3) = \sum_{i,j=1}^{3} k_{ij}\alpha_i\alpha_j, \quad k_{ji} = k_{ij} ,$$

divides each of the three linear functions Y_1, Y_2, Y_3 of $\alpha_1, \alpha_2, \alpha_3$, where

$$\text{(ii)} \qquad Y_i = \sum_{j=1}^{3} k_{ij}\alpha_j, \quad k_{ji} = k_{ij} , \ i = 1,2,3,$$

where the determinant associated with U is equal to zero, where all values of $\alpha_1, \alpha_2, \alpha_3$ are excluded such that $U(\alpha_1, \alpha_2, \alpha_3) = 0$, and where k_{ij}, $i,j = 1,2,3$, are given by

$$\text{(iii)} \qquad \begin{aligned}
k_{11} &= a_{22}X_{33}^2 + a_{33}X_{23}^2 - 2a_{23}X_{23}X_{33} \\
k_{12} &= -a_{12}X_{33}^2 - a_{33}X_{13}X_{23} + a_{13}X_{23}X_{33} + a_{23}X_{13}X_{33} \\
k_{13} &= -a_{13}X_{23}^2 - a_{22}X_{13}X_{33} + a_{12}X_{23}X_{33} + a_{23}X_{13}X_{23} \\
k_{22} &= a_{11}X_{33}^2 + a_{33}X_{13}^2 - 2a_{13}X_{13}X_{33} \\
k_{23} &= -a_{11}X_{23}X_{33} - a_{23}X_{13}^2 + a_{12}X_{13}X_{33} + a_{13}X_{13}X_{23} \\
k_{33} &= a_{11}X_{23}^2 + a_{22}X_{13}^2 - 2a_{12}X_{13}X_{23} .
\end{aligned}$$

Any indefinite form is excluded if $k_{11} = k_{12} = \cdots = k_{33} = 0$, or any set X_{13}, X_{23}, X_{33} if $\phi(X_{13}, X_{23}, X_{33}) = 0$, where ϕ is the adjoint form of f. Moreover, if (c_{jk}) exists, with $|c_{jk}| = 1$, then c_{12}, c_{22}, c_{32} are given by

$$\text{(iv)} \qquad \begin{aligned}
c_{12} &= X_{23}\gamma - X_{33}\beta \\
c_{22} &= X_{33}\alpha - X_{13}\gamma \\
c_{32} &= X_{13}\beta - X_{23}\alpha ,
\end{aligned}$$

<u>where</u> α, β, γ <u>are integral solutions of a pair of the equations</u>

(v)
$$h_1\alpha + h_2\beta + h_3\gamma = -1$$
$$B_{i1}\alpha + B_{i2}\beta + B_{i3}\gamma = 0, \ i = 1,2,3.$$

<u>Also</u> h_1, h_2, h_3 <u>are given by</u>

(vi)
$$h_1 = X_{23}\alpha_3 - X_{33}\alpha_2$$
$$h_2 = X_{33}\alpha_1 - X_{13}\alpha_3$$
$$h_3 = X_{13}\alpha_2 - X_{23}\alpha_1 \ .$$

<u>Further</u>, B_{ij}, $j = 1,2,3$, <u>are the elements of the matrix</u>

(vii)
$$M = \begin{pmatrix} h_1k_{12}-h_2k_{11} & h_1k_{22}-h_2k_{12} & h_1k_{23}-h_2k_{13} \\ h_1k_{13}-h_3k_{11} & h_1k_{23}-h_3k_{12} & h_1k_{33}-h_3k_{13} \\ h_2k_{13}-h_3k_{12} & h_2k_{23}-h_3k_{22} & h_2k_{33}-h_3k_{23} \end{pmatrix}.$$

<u>Finally</u>, c_{11}, c_{21}, c_{31} <u>are given by</u>

(viii)
$$c_{11} = X_{23}k - X_{33}n$$
$$c_{21} = X_{33}s - X_{13}k$$
$$c_{31} = X_{13}n - X_{23}s \ ,$$

<u>where</u> s, n, k <u>are integral solutions of the system</u>

(ix)
$$A\,s + B\,n + C\,k = 0$$
$$c_{12}s + c_{22}n + c_{32}k = -1,$$

<u>and where</u>

(x)
$$A = k_{11}\alpha + k_{12}\beta + k_{13}\gamma$$
$$B = k_{12}\alpha + k_{22}\beta + k_{23}\gamma$$
$$C = k_{13}\alpha + k_{23}\beta + k_{33}\gamma \ .$$

Although the above theorem was designed to determine whether a particular form f is equivalent to some general form f' having no cross-products, it can also be applied to the problem of ascertaining whether two particular forms are equivalent, and even more important, if they are equivalent, to the problem of finding the transformation sending one into the other. L. E. Dickson gives two indefinite forms

$$f = -x_1^2 + 2x_2^2 - 16x_3^2 + 2x_2x_3$$

and

$$f' = -y_1^2 - y_2^2 + 33y_3^2,$$

of determinant -33, and states that a transformation sending f into f' was found.[1] Such a transformation was sought for the purpose of tabulation of reduced, indefinite forms. Use of the preceding Theorem gives the result explicitly and with a minimum of work of the trial-and-error variety. By (3), $f_3 = b_{33}$, so that the values of c_{13}, c_{23}, c_{33} must cause f to represent 33. Take the values of the c_{i3} as 33, 29, and 8 respectively. Then $X'_{13} = -33$, $X'_{23} = 66$, and $X'_{33} = -99$ so that $g = 33 = b_{33}$, which satisfies Corollary 3. Hence by (6), $X_{13} = -1$, $X_{23} = 2$, and $X_{33} = -3$. By (iii), $k_{11} = -34$, $k_{12} = -29$, $k_{13} = -8$, $k_{22} = -25$, $k_{23} = -7$, and $k_{33} = -2$. Then

$$U = -34\alpha_1^2 - 25\alpha_2^2 - 2\alpha_3^2 - 58\alpha_1\alpha_2 - 16\alpha_1\alpha_3 - 14\alpha_2\alpha_3.$$

By (ii), $\quad Y_1 = -34\alpha_1 - 29\alpha_2 - 8\alpha_3$

---

[1] L. E. Dickson, Studies in the Theory of Numbers, p. 149.

$$Y_2 = -29\alpha_1 - 25\alpha_2 - 7\alpha_3$$
$$Y_3 = -8\alpha_1 - 7\alpha_2 - 2\alpha_3 .$$

The set of values $\alpha_1 = -1$, $\alpha_2 = 1$, $\alpha_3 = 1$ gives $U = -34 - 25 - 2 + 58 + 16 - 14 = -1$, or $|U| = 1$. Then $Y_1 = -3$, $Y_2 = -3$, $Y_3 = -1$. Thus $|U|$ divides each of Y_1, Y_2, and Y_3. But this is sufficient that $f \sim f'$; hence the elements of the transformation (c_{jk}) sending f into f' can be determined. By (vi),

$$h_1 = (\ 2)(\ 1) - (-3)(\ 1) = 5$$
$$h_2 = (-3)(-1) - (-1)(\ 1) = 4$$
$$h_3 = (-1)(\ 1) - (\ 2)(-1) = 1.$$

The elements of the first row of the matrix M of (vii) are

$$B_{11} = (\ 5)(-29) - (\ 4)(-34) = -9$$
$$B_{12} = (\ 5)(-25) - (\ 4)(-29) = -9$$
$$B_{13} = (\ 5)(-\ 7) - (\ 4)(-\ 8) = -3.$$

Then the system (v) of equations is

$$4\beta + \gamma = -5\alpha - 1, \qquad 3\beta + \gamma = -3\alpha$$

Employing Cramer's Rule,

$$\beta = -2\alpha - 1, \qquad \gamma = 3\alpha + 3.$$

Therefore,

$$\alpha = \alpha, \quad \beta = -2\alpha - 1, \quad \gamma = 3\alpha + 3,$$

and by (x),

$$A = -34(\alpha) - 29(-2\alpha - 1) - 8(3\alpha + 3) = 5$$

$$B = -29(\alpha) - 25(-2\alpha - 1) - 7(3\alpha + 3) = 4$$

$$C = -8(\alpha) - 7(-2\alpha - 1) - 2(3\alpha + 3) = 1.$$

The system (ix) is then

$$5s + 4n + k = 0$$

$$3s + 3n + k = -1,$$

to which Cramer's Rule is applied, yielding $n = 1 - 2s$, $k = 3s - 4$, $s = s$, where s is arbitrary. By (iv) the three c_{12} are computed and found to be

$$c_{12} = (2)(3\alpha + 3) - (-3)(-2\alpha - 1) = 3$$

$$c_{22} = (-3)(\alpha) - (-1)(3\alpha + 3) = 3$$

$$c_{32} = (-1)(-2\alpha - 1) - (2)(\alpha) = 1.$$

Finally the first column of (c_{jk}) is given by (viii).

$$c_{11} = (2)(3s - 4) - (-3)(1 - 2s) = -5$$

$$c_{21} = (-3)(s) - (-1)(3s - 4) = -4$$

$$c_{31} = (-1)(1 - 2s) - (2)(s) = -1.$$

Hence the transformation

$$(c_{jk}) = \begin{pmatrix} -5 & 3 & 33 \\ -4 & 3 & 29 \\ -1 & 1 & 8 \end{pmatrix}$$

carries f into f'. This is not, however, the exact transformation given by Dickson. Postmultiplication of (c_{jk}) by the automorph

$$\begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

of f' gives the transformation given by Dickson, namely,

$$\begin{pmatrix} 3 & 5 & 33 \\ 3 & 4 & 29 \\ 1 & 1 & 8 \end{pmatrix}.$$

Certain other changes of sign and interchanges of columns are possible, due to the nature of the form f', in that f' has no cross-product terms and has two coefficients equal.

In the process of finding the transformation (c_{jk}) sending f into f', a crucial point is the choice of the elements c_{13}, c_{23}, c_{33} of the transformation. In the transformation obtained above, the elements c_{i3} used were those given by Dickson. This choice is not at all arbitrary, for the c_{i3} must satisfy, by (3), $f_3 = b_{33}$, or in this case

(82) $$-c_{13}^2 + 2c_{23}^2 - 16c_{33}^2 + 2c_{23}c_{33} = 33.$$

Furthermore, Corollary 4 must be satisfied, so that c_{13} must be a multiple of b_{33}, since a_{11} equals -1. By (82), c_{13} cannot be even. Hence c_{13} is an odd multiple of b_{33}. The two conditions just mentioned are necessary conditions but are not sufficient; another condition is that there must exist columns c_{i1} and c_{i2}, $i = 1,2,3$, for which f_1 and f_2 equal b_{11} and b_{22} respectively. Finally, the determinant $|c_{jk}|$ must equal one.

Now if the choice one makes for the elements of the third column gives the third column of an actual transformation sending f into f', then the preceding Theorem will give the other elements of the transformation. Finding the third column elements remains largely a problem of trial and error.

An example is given here of a set c_{13}, c_{23}, c_{33} for which f_3 equals b_{33}, yet where there exists no possible choice of columns c_{i1} and c_{i2} causing f to be sent into f'. Apply to

$$f' = -y_1^2 - y_2^2 + 33y_3^2$$

the transformation

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}$$

to obtain an equivalent form

$$f'' = 33y_1^2 - y_2^2 - y_3^2 .$$

Now if there exists a transformation (d_{jk}) sending f into f', then there exists a transformation

$$(c_{jk}) = (d_{jk})\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}$$

which sends f into f". Conversely, if there exists a transformation (c_{jk}) sending f into f", then there exists a transformation

$$(d_{jk}) = (c_{jk})\begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

which carries f into f', for

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (I),$$

the identity transformation. One must seek, then, a transformation (c_{jk}) sending f into f''. The elements of the third column must satisfy $f_3 = b_{33}$, by (3), or

(83) $$-c_{13}^2 + 2c_{23}^2 - 16c_{33}^2 + 2c_{23}c_{33} = -1$$

An obvious choice of integers satisfying (83) is $c_{13} = 1$, $c_{23} = c_{33} = 0$. Then by (2),

$$X'_{13} = a_{11}c_{13} = -1$$
$$X'_{23} = a_{12}c_{13} = 0$$
$$X'_{33} = a_{13}c_{13} = 0 ,$$

so that $g = 1$, and therefore, $X'_{i3} = X_{i3}$, $i = 1,2,3$. By (1),

$$b_{13} = (-1)(c_{11}) + (\ 0)(c_{21}) + (\ 0)(c_{31}) = 0$$

If this last relation is to be satisfied, then $c_{11} = 0$. But since, by (3), b_{11} must equal f_1, or

$$f_1 = f(c_{11},c_{21},c_{31}) = -c_{11}^2 + 2c_{21}^2 - 16c_{31}^2 + 2c_{21}c_{31} = 33,$$

then an even integer equals an odd integer, a contradiction.

This illustrates that extreme care must be taken in choosing the elements of the third column so that the choice does not go beyond the realm of possibility.

Another pair of equivalent forms given by Dickson is given below, and the transformation will be found as before.[2]

$$f = -x_1^2 + 2x_2^2 - 28x_3^2 + 2x_2x_3$$
$$f' = -y_1^2 - y_2^2 + 57y_3^2$$

Again, by Corollary 4, c_{13} is a multiple of $b_{33} = 57$, and since c_{13} is odd, take $c_{13} = 57$. Then since $g = 57$ by Corollary 3, compute

$$X'_{13} = -57$$
$$X'_{23} = 2c_{23} + c_{33}$$
$$X'_{33} = c_{23} - 28c_{33} \quad ,$$

and use the resulting congruences

$$2c_{23} \equiv -c_{33} \pmod{57}$$
$$c_{23} \equiv 28c_{33} \pmod{57} .$$

By (3), $f(57, c_{23}, c_{33}) = 57$, so that

$$2c_{23}^2 - 28c_{33}^2 + 2c_{23}c_{33} = (57)^2 + 57$$

or
$$c_{23}^2 + c_{23}c_{33} - 14c_{33}^2 = 1653$$

from which it is easily determined that c_{23} must be odd and c_{33} even. The pair $c_{23} = 149$, $c_{33} = 44$ is discovered to sat-

[2] Ibid., p. 149.

isfy all the above requirements. Now $X'_{13} = -57$, $X'_{23} = 342$, $X'_{33} = -1083$, so that $g = 57$, and by (6), $X_{13} = -1$, $X_{23} = 6$, and $X_{33} = -19$. By (iii), $k_{11} = -58$, $k_{12} = -149$, $k_{13} = -44$, $k_{22} = -389$, $k_{23} = -115$, $k_{33} = -34$, and by (i),

$$- U = 58\alpha_1^2 + 389\alpha_2^2 + 34\alpha_3^2 + 298\alpha_1\alpha_2 + 88\alpha_1\alpha_3 + 230\alpha_2\alpha_3 .$$

By (ii),

$$\begin{aligned} - Y_1 &= 58\alpha_1 + 149\alpha_2 + 44\alpha_3 \\ - Y_2 &= 149\alpha_1 + 389\alpha_2 + 115\alpha_3 \\ - Y_3 &= 44\alpha_1 + 115\alpha_2 + 34\alpha_3 \quad . \end{aligned}$$

$U(0, 3, -10) = (-1)$; $Y_1(0, 3, -10) = 7$, $Y_2(0, 3, -10) = 17$, and $Y_3(0, 3, -10) = 5$. Hence by the Theorem of this chapter, since integers $\alpha_1 = 0$, $\alpha_2 = 3$, $\alpha_3 = -10$ exist for which $|U|$ divides each Y_i, $i = 1,2,3$, then the transformation (c_{jk}) of determinant one exists which carries f into f'. Then by (vi),

$$\begin{aligned} h_1 &= (\ 6)(10) - (-19)(-3) = 3 \\ h_2 &= (-19)(\ 0) - (\ -1)(10) = 10 \\ h_2 &= (\ -1)(-3) - (\ 6\ )(\ 0) = 3 . \end{aligned}$$

By (vii),

$$B_{11} = 133, \quad B_{12} = 323, \quad B_{13} = 95.$$

The system (v) becomes

$$\begin{aligned} 3\alpha + 10\beta + 3\gamma &= -1 \\ 7\alpha + 17\beta + 5\gamma &= 0. \end{aligned}$$

Solving by Cramer's Rule gives the three values

$$\alpha = \frac{-\gamma - 17}{-19}, \quad \beta = \frac{6\gamma + 7}{-19}, \quad \gamma = \gamma .$$

Then $\gamma \equiv -17 \pmod{19}$, or $\gamma = 19k + 2$, where k is arbitrary. Hence

$$\alpha = k + 1, \quad \beta = -6k - 1, \quad \gamma = 19k + 2.$$

By (iv), $c_{12} = -7$, $c_{22} = -17$, $c_{32} = -5$. By (x),

$$\begin{aligned} A &= -58(k+1) - 149(-6k-1) - 44(19k+2) = 3 \\ B &= -149(k+1) - 389(-6k-1) - 115(19k+2) = 10 \\ C &= -44(k+1) - 115(-6k-1) - 34(19k+2) = 3 , \end{aligned}$$

and the system (ix) is

$$\begin{aligned} 3s + 10n + 3k &= 0 \\ 7s + 17n + 5k &= 1 , \end{aligned}$$

which by Cramer's Rule gives, finally,

$$s = m + 1, \quad n = -6m - 3, \quad k = 19m + 9.$$

By (viii), $c_{11} = -3$, $c_{21} = -10$, $c_{31} = -3$. Then the transformation

$$\begin{pmatrix} -3 & -7 & 57 \\ -10 & -17 & 149 \\ -3 & -5 & 44 \end{pmatrix}$$

carries f into f'. In obtaining this particular transformation, the values used for α_1, α_2, and α_3 were 0, -3, and -10, respectively. The choice of 0, -3, and 10 would have been equally appropriate and would have resulted in the slightly different transformation

$$\begin{pmatrix} 3 & 7 & 57 \\ 10 & 17 & 149 \\ 3 & 5 & 44 \end{pmatrix}.$$

It is the latter transformation which is given by Dickson.

CHAPTER VII

APPLICATIONS TO THE THEORY OF TABULATION OF AUTOMORPHS

Given any form f there exists at least one transformation sending the form f into itself. Such a transformation is called an <u>automorph</u> of f. In the study of whether a form f is equivalent to some form f', it is often quite useful to know the automorphs of the form f or of the form f'. This is true because given one transformation of f into f', one can find all such transformations of f into f', if all the automorphs of f (or of f') are known.[1]

In studying the automorphs of the form f' of Chapter VI, an immediate corollary of the Theorem of E. H. Hadlock of that chapter is useful.

COROLLARY. <u>A necessary and sufficient condition that the forms</u> $f = a_{11}x_1^2 + a_{22}x_2^2 + a_{33}x_3^2$ <u>and</u> $f' = b_{11}y_1^2 + b_{22}y_2^2 + b_{33}y_3^2$ <u>be equivalent is that there exist integral values of</u> α_1, α_2, α_3 <u>for which</u> $|U|$ <u>divides each</u> Y_i, $i = 1,2,3$, <u>where</u> $|U|$ <u>is defined by (i),</u> Y_i <u>by (ii), and</u> k_{ij}, $i, j = 1, 2, 3$, <u>by</u>

---

[1] L. E. Dickson, <u>History of the Theory of Numbers</u>, III, 210.

$$(84)\qquad \begin{aligned} k_{11} &= a_{22}X_{33}^{2} + a_{33}X_{23}^{2} \\ k_{12} &= -a_{33}X_{13}X_{23} \\ k_{13} &= -a_{22}X_{13}X_{33} \\ k_{22} &= a_{11}X_{33}^{2} + a_{33}X_{13}^{2} \\ k_{23} &= -a_{11}X_{23}X_{33} \\ k_{33} &= a_{11}X_{23}^{2} + a_{22}X_{13}^{2}\ . \end{aligned}$$

Consider the positive form $f = a_{11}x_1^{2} + a_{22}x_2^{2} + a_{33}x_3^{2}$, where $0 < a_{33} \leq a_{22} \leq a_{11}$. In computing the automorphs of f, one seeks all transformations (c_{jk}) sending f into $f' = f$, so that $a_{ii} = b_{ii}$, $a_{ij} = b_{ij} = 0$, $i \neq j$, $i, j = 1,2,3$. It is necessary, by (3), that $f_3 = b_{33} = a_{33}$, and all sets of integers c_{13}, c_{23}, c_{33} such that $f(c_{13}, c_{23}, c_{33}) = a_{33}$, if $a_{33} < a_{22} < a_{11}$, are given by 0,0,1 and 0,0,-1.

When $c_{13} = 0$, $c_{23} = 0$, $c_{33} = 1$, then by (2), $X'_{13} = X'_{23} = 0$, $X'_{33} = a_{33}$; thus $g = a_{33}$, $X_{13} = X_{23} = 0$, $X_{33} = 1$. Therefore, by (84), $k_{11} = a_{22}$, $k_{22} = a_{11}$, and $k_{12} = k_{13} = k_{23} = k_{33} = 0$. By (i) and (ii),

$$U = a_{22}\alpha_1^{2} + a_{11}\alpha_2^{2}$$

and $\quad Y_1 = a_{22}\alpha_1\ ,\ Y_2 = a_{11}\alpha_2\ ,\ Y_3 = 0.$

It is required that each Y_i/U be an integer. Since Y_3 is the integer zero, then the only requirements are that Y_1/U and Y_2/U be integers. This last condition is true if and only if either $\alpha_1 = 0$, $\alpha_2 = \pm 1$ or $\alpha_1 = \pm 1$, $\alpha_2 = 0$, for if

$|\alpha_1| > 1$, then $\alpha_1^2 > |\alpha_1|$, $a_{22}\alpha_1^2 > a_{22}|\alpha_1|$,

and hence

$$a_{22}\alpha_1^2 + a_{11}\alpha_2^2 > a_{22}|\alpha_1|,$$

so that
$$\frac{a_{22}\alpha_1}{a_{22}\alpha_1^2 + a_{11}\alpha_2^2}$$

is not integral. Similarly, if $|\alpha_2| > 1$, then $|U|$ does not divide Y_2. Therefore it is observed that when $c_{13} = 0$, $c_{23} = 0$, $c_{33} = 1$, then either of two cases occur. Case (1) comprises the values $\alpha_1 = 0$, $\alpha_2 = \pm 1$, $\alpha_3 = \alpha_3$, and case (2), the values $\alpha_1 = \pm 1$, $\alpha_2 = 0$, $\alpha_3 = \alpha_3$.

By (vi), case (1) gives $h_1 = \mp 1$, $h_2 = h_3 = 0$. By (vii), $B_{11} = 0$, $B_{12} = \mp a_{11}$, $B_{13} = 0$. The system (v) yields $\alpha = \pm 1$, $\beta = 0$, $\gamma = \gamma$. Then the values of A, B, C, by (x), are $A = \pm 1$, $B = 0$, $C = 0$. The system (ix) is $s = 0$, $n = \pm 1$, $k = k$, so that $c_{12} = 0$, $c_{22} = \pm 1$, $c_{32} = 0$. Finally, $c_{11} = 1$, $c_{21} = c_{31} = 0$.

Case (2) gives, by the same method, the values $h_1 = 0$, $h_2 = \pm 1$, $h_3 = 0$; $B_{11} = \mp a_{22}$, $B_{12} = B_{13} = 0$. $\alpha = 0$, $\beta = \mp 1$, $\gamma = \gamma$; $c_{12} = \pm 1$, $c_{22} = c_{32} = 0$. Continuing this process, $c_{11} = 0$, $c_{21} = \mp 1$, $c_{31} = 0$. The transformations just obtained, namely, those of case (2) are not automorphs of $f = a_{11}x_1^2 + a_{22}x_2^2 + a_{33}x_3^2$, $a_{11} > a_{22} > a_{33}$, for by (3), $f_2 = a_{11} \neq a_{22}$.

Taking the second set of values for the c_{i3}, $i = 1, 2, 3$, i.e., $c_{13} = 0$, $c_{23} = 0$, $c_{33} = -1$, then $X'_{13} = 0$, $X'_{23} = 0$,

$X'_{33} = -a_{33}$. Hence $g = a_{33} > 0$, so that $X_{13} = 0$, $X_{23} = 0$, $X_{33} = -1$. By (84), $k_{11} = a_{22}$, $k_{22} = a_{11}$, $k_{12} = k_{13} = k_{23} = k_{33} = 0$. The only values for α_1, α_2, and α_3 are, case (3), $\alpha_1 = 0$, $\alpha_2 = \pm 1$, $\alpha_3 = \alpha_3$, and, case (4), $\alpha_1 = \pm 1$, $\alpha_2 = 0$, $\alpha_3 = \alpha_3$.

Case (3) yields $c_{11} = \mp 1$, $c_{21} = c_{31} = 0$; $c_{22} = \pm 1$, $c_{12} = c_{32} = 0$. The transformations made up of those elements constitute automorphs of f, as can be established by subjecting f to the transformations.

Case (4) yields no automorph of f, for the values obtained, $c_{11} = 0$, $c_{21} = \mp 1$, $c_{31} = 0$, $c_{12} = \mp 1$, $c_{22} = c_{32} = 0$, give transformations which, by (3), give $f_2 = a_{11} \neq a_{22}$.

Hence all sets c_{i3} have been obtained satisfying $f_3 = b_{33}$; all sets α_i were found satisfying $|U| \,\big|\, Y_i$, $i = 1,2,3$; thus all transformations sending f into itself have been exhibited. They may be written in matrix form as follows. From case (1), two such automorphs are

$$A_1: \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad A_2: \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

From case (3), two additional automorphs A_3 and A_4 are given by

$$A_3: \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \qquad A_4: \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

When transformations A_1, A_2, A_3, and A_4 are applied to the form f, they are found to be automorphs of f.

The four transformations obtained which are not automorphs of f, when $a_{11} > a_{22} > a_{33}$, namely, those of case (2),

$$A_5: \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } A_6: \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

and those of case (4),

$$A_7: \begin{pmatrix} 0 & -1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} \text{ and } A_8: \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix},$$

send f into the equivalent form

$$f' = a_{22}y_1^2 + a_{11}y_2^2 + a_{33}y_3^2.$$

Therefore in the case of a form f having $a_{22} = a_{11}$, for example the form $f = 2x_1^2 + 2x_2^2 + x_3^2$, then f has the additional four automorphs A_5, A_6, A_7, and A_8.

Consider now the form f with $a_{11} > a_{22} = a_{33}$. Then $f_3 = b_{33}$ is satisfied by the sets c_{13}, c_{23}, c_{33} respectively, 0, 0, 1; 0, 0, -1; 0, 1, 0; and 0, -1, 0. The former two sets of values have already been employed to obtain automorphs A_1, A_2, A_3, and A_4. The third set of values, 0, 1, and 0, will be investigated next.

When $c_{13} = 0$, $c_{23} = 1$, $c_{33} = 0$, then $X'_{13} = 0$, $X'_{23} = a_{22}$, $X'_{33} = 0$, and $g = a_{22}$. By (84), $k_{11} = a_{33}$, $k_{33} = a_{11}$,

and $k_{12} = k_{13} = k_{22} = k_{23} = 0$. Then

$$U = a_{33}\alpha_1^{\;2} + a_{11}\alpha_3^{\;2}, \quad Y_1 = a_{33}\alpha_1, \; Y_2 = 0, \; Y_3 = a_{11}\alpha_3.$$

The two resulting sets of values for the α_i, $i = 1,2,3$, are given by case (5), $\alpha_1 = 0$, $\alpha_2 = \alpha_2$, $\alpha_3 = \pm 1$, and case (6), $\alpha_1 = \pm 1$, $\alpha_2 = \alpha_2$, $\alpha_3 = 0$.

Case (5) gives the following values: $h_1 = \pm 1$, $h_2 = h_3 = 0$; $B_{21} = B_{22} = 0$, $B_{23} = \pm 1$, $c_{12} = c_{22} = 0$, $c_{32} = \pm 1$, $c_{11} = \mp 1$, $c_{21} = 0$, and $c_{31} = 0$.

Case (6), after similar computation, yields $c_{11} = 0$, $c_{21} = 0$, $c_{31} = \mp 1$, $c_{12} = \mp 1$, $c_{22} = 0$, and $c_{32} = 0$.

The transformations given by case (5) are

$$A_9: \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \text{ and } A_{10}: \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix},$$

and those of case (6) are

$$A_{11}: \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ -1 & 0 & 0 \end{pmatrix} \text{ and } A_{12}: \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Only A_9 and A_{10} are automorphs of f when $a_{11} > a_{22} = a_{33}$, for A_{11} and A_{12} send f into

$$f' = a_{33}y_1^{\;2} + a_{11}y_2^{\;2} + a_{22}y_3^{\;2}.$$

When $c_{13} = 0$, $c_{23} = -1$, and $c_{33} = 0$, four new transformations arise as follows:

$$A_{13}: \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}, \quad A_{14}: \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix},$$

$$A_{15}: \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}, \quad A_{16}: \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{pmatrix}.$$

Of these only the first two are automorphs of f when $a_{11} > a_{22} = a_{33}$. Hence when f is so restricted, all automorphs of f are given by A_1, A_2, A_3, A_4, A_8, A_{10}, A_{13}, and A_{14}.

Finally the form f will be considered when all of its non-zero coefficients are equal, i.e., $a_{11} = a_{22} = a_{33}$. Then other possible values for the c_{13} are 1, 0, 0 and -1, 0, 0.

When $c_{13} = 1$, $c_{23} = c_{33} = 0$, then $X'_{13} = a_{11}$, $X'_{23} = X'_{33} = 0$; $g = a_{11} = a_{22} = a_{33}$, $X_{13} = 1$, $X_{23} = 0$, and $X_{33} = 0$. Then $k_{11} = k_{12} = k_{13} = k_{23} = 0$; $k_{22} = a_{33}$, $k_{33} = a_{22}$, so that either $\alpha_1 = \alpha_1$, $\alpha_2 = 0$, $\alpha_3 = \pm 1$, or $\alpha_1 = \alpha_1$, $\alpha_2 = \pm 1$, $\alpha_3 = 0$. These cases yield four automorphs of f, namely,

$$A_{17}: \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad A_{18}: \begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix},$$

$$A_{19}: \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 0 \end{pmatrix}, \quad A_{20}: \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

The final set of values, $c_{13} = -1$, $c_{23} = c_{33} = 0$, completes all transformations obtained in this manner; the results are

$$A_{21}: \begin{pmatrix} 0 & 0 & -1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \qquad A_{22}: \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix},$$

$$A_{23}: \begin{pmatrix} 0 & 0 & -1 \\ -1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \qquad A_{24}: \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}.$$

All automorphs of the positive form f have now been derived. They are listed in Table 1 on the following page. The number of automorphs of f, i.e., four, eight, or twenty-four, agrees with a statement of L. E. Dickson.[2] The results of Table 1 are not original but are presented as an illustration of this original method of obtaining automorphs. The method so illustrated is applicable to any form having all of its cross-products equal to zero but seems to be more successful in applications to positive forms. Since there is at least one reduced form with all cross-products equal to zero of any determinant $d \neq 0$, then the method is applicable to a multitude of forms.

The value of knowing all automorphs of f is illustrated as follows. Consider the two equivalent forms

---

[2]L. E. Dickson, Studies in the Theory of Numbers, p. 180.

TABLE 1

AUTOMORPHS OF THE POSITIVE

FORM $f = \sum_{i=1}^{3} a_{ii}x_i^2$

Restrictions on the Coefficients of f	Number of Automorphs	Automorphs of the Form f
$a_{11} > a_{22} > a_{33}$	4	A_1, A_2, A_3, A_4
$a_{11} = a_{22} > a_{33}$	8	$A_1, A_2, A_3, A_4, A_5, A_6, A_7, A_8$
$a_{11} > a_{22} = a_{33}$	8	$A_1, A_2, A_3, A_4, A_9, A_{10}, A_{13}, A_{14}$
$a_{11} = a_{22} = a_{33}$	24	$A_1, \ldots, A_{24}$

$$f = 3x_1^2 + 20x_2^2 + 2x_3^2 + 12x_2x_3$$

and $$f' = 3y_1^2 + 2y_2^2 + 2y_3^2.$$

Since $f_3 = 2$ when $c_{13} = 0$, $c_{23} = 0$, $c_{33} = 1$, then $X'_{13} = 0$, $X'_{23} = 6$, $X'_{33} = 2$; $g = 2$, $X_{13} = 0$, $X_{23} = 3$, and $X_{33} = 1$. By (iii), $k_{11} = k_{12} = 0$, $k_{13} = k_{22} = 3$, $k_{23} = -9$, $k_{33} = 27$. By (i) and (ii),

$$U = 3\alpha_2^2 + 27\alpha_3^2 + 6\alpha_1\alpha_3 - 18\alpha_2\alpha_3$$

$$Y_1 = 3\alpha_3^2$$

$$Y_2 = 3\alpha_2^2 - 9\alpha_3^2$$

$$Y_3 = -9\alpha_2^2 + 27\alpha_3^2 .$$

Then let $\alpha_1 = 0$, $\alpha_2 = 1$, $\alpha_3 = 0$; then $U = 3$, $Y_1 = 0$, $Y_2 = 3$, $Y_3 = -9$, so that $|U|$ divides each of the three Y_i, $i = 1, 2, 3$. By (vi), $h_1 = -1$, $h_2 = h_3 = 0$, and by (vii), $B_{11} = 0$, $B_{12} = -3$, $B_{13} = 9$; then $\alpha = 1$, $\beta = 3\gamma$, $\gamma = \gamma$, so that $c_{12} = 0$, $c_{22} = 1$, $c_{32} = -3$. By (x), $A = 1$, $B = C = 0$. The system (ix) is $s = 0$, $n - 3k = -1$, and finally $c_{11} = 1$, $c_{21} = 0$, and $c_{31} = 0$. Thus one transformation sending f into f' is

$$C_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -3 & 1 \end{pmatrix}.$$

Now all transformations sending f into f' can be obtained by the use of automorphs. By Table 1, all automorphs of f' are A_1, A_2, A_3, A_4, A_9, A_{10}, A_{13}, and A_{14}. Hence all transformations C_i carrying f into f' are given by

$$C_i = C_1A_i\ ,\ i = 1, 2, 3, 4, 9, 10, 13, 14.$$

Naturally the actual computation is expedited by the use of matrix multiplication. The result of this work is given below.

$$C_1: \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -3 & 1 \end{pmatrix} \qquad C_2: \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 3 & 1 \end{pmatrix}$$

$$C_3: \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -3 & -1 \end{pmatrix} \qquad C_4: \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 3 & -1 \end{pmatrix}$$

$$C_9: \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & -3 \end{pmatrix} \qquad C_{10}: \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & -3 \end{pmatrix}$$

$$C_{13}: \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 3 \end{pmatrix} \qquad C_{14}: \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 3 \end{pmatrix}$$

Evidently this type of computation, by the use of automorphs, is much more rapid than direct computation by the method of Chapter VI. However, in order to use this automorphic method, at least one C_i must be known. And it is this problem, the problem of finding one transformation sending a form into another form, which sometimes calls for every device at ones disposal. To this problem the method of Chapter VI is applicable.

CHAPTER VIII

SUMMARY

The first six chapters of this dissertation concern the results of investigations on the subject of equivalence of ternary quadratic forms of determinant $d \neq 0$. Various restrictions are placed on the coefficients of f', and necessary and/or sufficient conditions that a general form f be equivalent to f' are sought. The resulting conditions are stated in concise language as theorems, lemmas, and corollaries. Since any condensation of these statements would but result in omission of necessary parts of them, no such condensation is attempted in this summary. However, it is thought that a brief reference table of the more useful portions of the dissertation may be helpful to a student wishing to use the results in determining whether two given forms are equivalent. Such a tabular index is presented on the following pages as Table 2.

In using Table 2, one should first observe whether the given form f' is described in the first column, and, if not, one should employ suitable interchanges of variables to obtain, if possible, a form which is described in column one and which is equivalent to f'. All such possible interchanges

TABLE 2

SUMMARY OF CONDITIONS THAT A FORM f OF DETERMINANT d $\neq$ 0 BE EQUIVALENT TO A FORM f'

Restrictions on the Coefficients of the Form f'	Conditions[a] for Equivalence of f and f'	References[b]
(I) $b_{13} = 0$, $b_{23} = Kb_{33}$, where K is any integer	n.a.s: that f represent primitively g or -g.	Lem. 3, p. 9.
	n.: that $g = \lvert b_{33} \rvert$.	Cor. 3, p. 15.
	s.: that f represent one primitively.	Cor. 1, p. 14.
	n.: that f represent primitively a divisor of d.	Th. 1, p. 16.
	n.a.s: that $g\phi(X_{13}, X_{23}, X_{33}) = d$ or $-d$.	Th. 2, p. 19.
(II) $b_{13} = 0$	Any form f is equivalent to some form f'	Th. 7, p. 62.

[a]Conditions are indicated as necessary, sufficient, or necessary and sufficient by the abbreviations, n., s., and n.a.s.

[b]References in the Table are to various statements in this dissertation; abbreviations for Lemma, Theorem, and Corollary are Lem., Th., and Cor., respectively.

TABLE 2--Continued

Restrictions on the Coefficients of the Form f'	Conditions for Equivalence of f and f'	References
(III) $b_{13} = 0$, $b_{23} = 0$	n.a.s.: that f represent primitively g or -g.	Cor. 2, p. 14.
	n.: that $g = \|b_{33}\|$	Cor. 3, p. 15.
(IV) $b_{23} = 0$, $b_{13} = N$, where N is any integer	n.a.s.: that the g.c.d. of the three constants (47) divide g.	Lemma 5, p. 45.
	s.: that the g.c.d. of the three constants, $Nc_{i3}-f_3c_{i1}$, $i=1,2,3$, divide g.	Cor. 5, p. 50.
(V) $b_{12} = N$, where N is any integer	Any properly primitive form f is equivalent to some form f'.	Conjecture, p. 66.
(VI) $b_{13} = N$, $b_{23} = 0$, $b_{33} = 1$	s.: that f be properly primitive and represent one primitively.	Th. 8, p. 69.
(VII) $b_{13} = 1$, $b_{23} = 0$, $b_{33} = 1$	s.: that f be properly primitive and represent one primitively.	Cor. 6, p. 70.

TABLE 2--Continued

Restrictions on the Coefficients of the Form f'	Conditions for Equivalence of f and f'	References
(VIII) $b_{13} = 0$, $b_{23} = M$, where M is any integer	See discussion of Chapter V.	Chapter V, pp. 74-75.
(IX) $b_{ii} = A$, $i = 1, 2$, or 3, and where A is any integer	n.: that f represent A primitively.	Remarks, p. 18.
	s.: that f represent A primitively.	Lem. 7, p. 54.
(X) $b_{12} = b_{13} = b_{23} = 0$	n.: that f represent primitively a divisor of d.	Th., p. 76.
	n.: that f represent primitively g or $-g$.	Th., p. 76.
	n.a.s.: that there exist integers α_1, α_2, and α_3 for which the value of $\lvert U \rvert$ divides Y_1, Y_2, and Y_3.	Th., p. 76.

greatly increase the utility of the table. Two further suggestions were made in Chapter V: (1) if no theorem, lemma, or corollary seems to apply to the form f' in question, interchange f and f'; and (2) if the problem is still unresolved, investigate whether the adjoint forms ϕ and ϕ' of f and f', respectively, are equivalent, for adjoints of equivalent forms are equivalent. Finally a word of caution seems appropriate that the material in Table 2 should be regarded more as an index than as a summary, for only in the statements of the propositions are the conditions for equivalence completely stated.

Incidental to the study of equivalence two additional items presented themselves, a study of certain Diophantine equations and an introduction to the theory of non-classic forms. The linear, non-homogeneous Diophantine equation in three variables was solved and shown always to possess a primitive solution. Also, given three linear functions in three indeterminates, with certain restrictions upon the coefficients of the functions, integral values for the indeterminates were shown to exist for which the g.c.d. of the values of the three functions is one. This completes the summary of the first six chapters.

Chapter VII consists of the application of some of the material of this dissertation to the direct computation of automorphs. A new method is illustrated whereby automorphs may be obtained. The method is applied to the posi-

tive form with no terms of type $2a_{ij}x_ix_j$, $i \neq j$, $i,j = 1, 2, 3$. The importance of automorphs is briefly discussed.

BIBLIOGRAPHY

Cahen, E. Theorie des Nombres. 2 vols. Paris: Librairie Scientifique A. Hermann & Fils, 1924.

Carmichael, Robert D. Diophantine Analysis. London: Chapman and Hall, Limited, 1915.

Dickson, Leonard E. History of the Theory of Numbers. Vol. III, Quadratic and Higher Forms. Washington: Carnegie Institution of Washington, 1923.

________. Introduction to the Theory of Numbers. Chicago: University of Chicago Press, 1929.

________. Modern Elementary Theory of Numbers. Chicago: University of Chicago Press, 1939.

________. Studies in the Theory of Numbers. Chicago: University of Chicago Press, 1930.

Glaisher, J. W. L. (ed.). The Collected Mathematical Papers of Henry John Stephen Smith. 2 vols. Oxford: The Clarendon Press, 1894.

Hadlock, E. H. Ternary Quadratic Forms Equivalent to Forms with One Term of Type $2b_{ij}y_iy_j$, $j \neq i$, (Paper read at the four hundred ninety-sixth meeting of the American Mathematical Society, Spartanburg, S. C., November, 1953). Abstract published in Bulletin of the American Mathematical Society, Vol. 60, No. 1, 1954.

Hardy, G. H., and Wright, E. M. An Introduction to the Theory of Numbers. Oxford: The Clarendon Press, 1938.

Jones, Burton W. The Arithmetic Theory of Quadratic Forms. Carus Mathematical Monograph Number Ten. Baltimore: The Mathematical Association of America, Waverly Press, 1950.

________. A Table of Eisenstein-reduced Positive Ternary Quadratic Forms of Determinant $\leq$ 200. Washington: National Academy of Sciences, 1935.

Lehmer, Derrick H. Guide to Tables in the Theory of Numbers. Washington: National Academy of Sciences, 1941.

Nagell, Trygve. Introduction to Number Theory. Stockholm; Almqvist & Wiksell, 1951.

Sagen, Oswald Karl. The Integers Represented by Sets of Positive Ternary Quadratic Non-classic Forms, Ph. D. dissertation, private edition, distributed by University of Chicago Libraries. Chicago; University of Chicago, 1936.

Skolem, Thoralf. Diophantische Gleichungen. New York; Chelsea Publishing Company, 1950.

BIOGRAPHICAL SKETCH

Thomas R. Horton was born on November 17, 1926, in Fort Pierce, Florida. He graduated from The Bolles School in Jacksonville, Florida, in 1944, at which time he enlisted in the Army of the United States. In 1946 Technical Sergeant Horton was honorably discharged. His undergraduate studies were begun at North Georgia College, continued at the University of Minnesota, and concluded at John B. Stetson University, where he received the degree Bachelor of Science with a major in mathematics in June, 1949. During the summer of 1949 Mr. Horton attended the University of Wisconsin, and the following year he continued graduate study in mathematics at the University of Florida. In July of 1950 he received the degree of Master of Science from the latter school. From September, 1950, until August, 1952, he was employed by The Bolles School in Jacksonville and during the second year was Commandant of the School. During the academic years 1952-53 and 1953-54 he pursued further graduate studies at the University of Florida and served as a graduate assistant in the Department of Mathematics, teaching various freshman mathematics courses. In the summer of 1954 he held the Dudley Beaumont Memorial Fellowship. Mr. Horton is a member of the Mathematical Association of America and of the American Mathematical Society.

This dissertation was prepared under the direction of the chairman of the candidate's supervisory committee and has been approved by all members of the committee. It was submitted to the Dean of the College of Arts and Sciences and to the Graduate Council and was approved as partial fulfillment of the requirements for the degree of Doctor of Philosophy.

August 9, 1954

C. F. Byers
Dean, College of Arts and Sciences

Dean, Graduate School

SUPERVISORY COMMITTEE:

E. H. Hodlich
Chairman

W. R. Hutcherson

F. W. Kokomoor

Z. M. Pirenian

Robert D. [illegible]